

User Guide

NL1901ACV Enhanced Hybrid 4G LTE Gateway



Important Notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the NetComm common identifier and device name to transmit or receive such data.

Safety and Hazards



Warning – Do not connect or disconnect cables or devices to or from the USB port, SIM card tray, Ethernet port or the terminals of the Molex power connector in hazardous locations such as those in which flammable gases or vapours may be present, but normally are confined within closed systems; are prevented from accumulating by adequate ventilation; or the location is adjacent to a location from which ignitable concentrations might occasionally be communicated.

Copyright

Copyright© 2018 NetComm Limited. All rights reserved.

The information contained herein is proprietary to NetComm. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm.

Trademarks and registered trademarks are the property of NetComm Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.



Note – This document is subject to change without notice.

Save our environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with domestic waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Document history

This document covers the following product:

NetComm Wireless NL1901ACV Enhanced Hybrid 4G LTE Gateway

VER.	DOCUMENT DESCRIPTION	DATE
v 1.0	Initial version.	December 2018

Table i. - Document revision history

Contents

Overview	8
Introduction	8
Target audience	8
Prerequisites	8
Notation	8
Welcome	9
Product overview	9
Package contents	9
Product features	10
Perfect for	10
Key Features	10
nbn and UFB ready	10
Undisrupted connectivity	10
Triple play services	10
Enhanced wireless experience	10
Media sharing	11
Physical dimensions and weight	11
NL1901ACV Default Settings	11
Interfaces	13
Front	13
Rear	15
Left Side	17
Safety and product care	18
Transport and handling	18
Installation and configuration of the NL1901ACV	19
Placement of your NL1901ACV	19
Avoiding obstacles and interference	19
Cordless phones	19
Choosing the "quietest" channel for your wireless network	20
Hardware installation	21
Connecting a client via Ethernet cable	21
Connecting a client wirelessly	21
First-time setup wizard	22
Select WAN Connection Type	22
ADSL	23
VDSL	25
Ethernet WAN	27
Mobile Network	30
Device Info	32
Summary	32

Device Info	32
WAN Connection Status	33
Cellular Network Connection Status	34
WAN	35
Statistics	36
Statistics – LAN	36
Statistics – WAN Service	36
Statistics – xTM	37
Statistics – xDSL	38
Route	39
ARP	39
DHCP	39
CPU & Memory	40
Advanced Setup	41
Layer 2 Interface	41
ATM Interface	41
PTM Interface	42
ETH Interface	43
WAN Service	44
PPP over Ethernet	45
IP over Ethernet	46
Bridging	47
Mobile Broadband	47
Add/Edit Mobile Broadband Setup	48
PIN settings	50
LAN	51
IPv4 Autoconfig	51
IPv6 Autoconfig	53
LAN VLAN Setting	54
NAT	55
Virtual Servers	55
Port Triggering	56
DMZ Host	57
ALG	58
Security	59
IP Filtering	59
MAC Filtering	61
Parental Control	62
Time Restriction	62
URL Filter	63
Quality of Service	65
QoS Queue	65
QoS Classification	67
QoS Port Shaping	67
Routing	69
Default Gateway	69
Static Route	69
Policy Routing	70
RIP	71
DNS	72
DNS Server Configuration	72
Dynamic DNS	73
DSL	74
DSL Advanced settings	75
ADSL Tone Settings	76
UPnP	76
DNS Proxy	77
DLNA	77
Storage Service	78

Storage Device Info	78
User Accounts.....	78
Interface Grouping.....	79
IP Tunnel.....	80
IPv6inIPv4	80
IPv4inIPv6	80
IPSec	81
Multicast (IGMP Configuration)	83
Wireless.....	85
WiFi 2.4GHz/WiFi 5GHz	85
Wireless – Basic.....	86
Wireless – Security	87
Wireless – MAC Filter	88
Wireless – Wireless Bridge (Wireless Distribution Service)	89
Wireless – Advanced.....	90
Wireless – Station Info	94
Voice.....	95
VoIP Status	95
SIP Basic Setting.....	96
SIP Advanced Setting	98
Configuring a VoIP dial plan.....	101
Dial plan syntax	101
Dial plan example: Australia Dial Plan	102
SIP Extra Setting.....	102
SIP Star Code Setting	103
SIP Debug Setting.....	103
VoIP Functionality.....	104
Registering	104
Placing a Call	104
Anonymous call	104
Do Not Disturb (DND)	105
Call Return.....	105
Call Hold.....	105
Call Waiting.....	105
Call Transfer.....	105
Consultative Transfer.....	106
Call Forwarding No Answer	106
Call Forwarding Busy.....	106
Call Forwarding All.....	106
Three-Way Conference	106
T.38 Faxing.....	107
Pass-Through Faxing	107
Diagnostics.....	108
Diagnostics – Diagnostics	108
Diagnostics – Ethernet OAM.....	110
Diagnostics – Ping.....	111
Diagnostics – Traceroute	111
Diagnostics – Start/Stop DSL.....	111
Management.....	112
Management – Settings	112
Backup	112
Update Settings.....	112
Factory Reset	113
Management – System Log	113
Configure Log Output.....	113

View System Log	115
Management – Security Log	116
Management – SNMP Agent	117
Management – TR-069 Client	118
Management – Internet Time	119
Management – Access Control	120
Passwords	120
Access List	121
Services Control	122
Management – Update Firmware	123
Management – Reboot	123
Logout	124
Reconnect	124
Additional Product Information	125
Establishing a wireless connection	125
Windows 7	125
Windows 8/8.1/10	125
Mac OSX 10.6	125
Troubleshooting	126
Using the indicator lights (LEDs) to Diagnose Problems	126
Power LED	126
Web Configuration	126
Login Username and Password	127
WLAN Interface	127
Appendix: Quality of Service setup example	128
Reserving IP addresses	128
QoS Configuration Settings	130
High Priority QoS Queue Configuration	130
Low Priority QoS Queue Configuration	131
High Priority QoS Classification	132
Low Priority QoS Classification	134
Limiting the upstream rate	136
Limiting the downstream rate	137
Table of Figures	139
Table of Tables	142
Legal & Regulatory Information	143
Intellectual Property Rights	143
Customer Information	143
Consumer Protection Laws	144
Product Warranty	144
Limitation of Liability	145
Contact	146

Overview

Introduction




This manual provides information related to the installation, operation, and use of the NL1901ACV.

Target audience

The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NL1901ACV, please confirm that you meet the minimum system requirements below.

-  An activated ADSL/VDSL or pre-configured WAN connection.
-  A computer with a working Ethernet adapter or wireless 802.11a/b/g/n/ac capability and the TCP/IP Protocol installed.
-  A current version of a web browser such as Internet Explorer®, Mozilla Firefox® or Google Chrome™.

Notation

The following symbols are used in this manual:



Note – The following note provides useful information.



Attention – The following situation requires attention.



Warning – The following note provides a warning.

Welcome

Thank you for purchasing a NetComm NL1901ACV. This guide contains all the information you need to configure your device.

Product overview

- 📶 Fully featured hybrid LTE/ DSL gateway
- 📶 VDSL2/ ADSL2+
- 📶 Embedded 4G LTE Cat 4 / 3G module
- 📶 1x Gigabit Ethernet WAN port
- 📶 New generation 802.11 AC1600, dual band concurrent WiFi - designed to provide a powerful wireless network
- 📶 2x WPS push buttons for the quick and easy connection of wireless devices on both 2.4GHz and 5GHz bands
- 📶 Internal SIM card slot
- 📶 VoIP for HD quality voice calls - connect up to 2 telephones
- 📶 4 x Gigabit Ethernet 10/100/1000 LAN ports
- 📶 2 x USB 2.0 ports
- 📶 Device performance monitoring and management through TR-069

Package contents

The NL1901ACV package consists of:

- 📶 1 x NetComm NL1901ACV Enhanced Hybrid 4G LTE Gateway
- 📶 2 x 4G/LTE antennas
- 📶 1 x RJ45 Ethernet cable
- 📶 1 x RJ11 Telephone cable
- 📶 1 x Power supply (12V/2A)
- 📶 1 x WiFi Security card
- 📶 1 x Warranty card
- 📶 1 x Quick Start Guide

If any of these items are missing or damaged, please contact NetComm Support immediately by visiting the NetComm Support website at: <https://support.netcommwireless.com/>

Product features

Perfect for

- 📶 Ultra-fast connection to nbn™ or UFB fibre networks
- 📶 High-speed connection to VDSL2/ ADSL2+ networks
- 📶 Fast 4G LTE back up connection
- 📶 Small to medium enterprises looking for reliable “always on” connectivity
- 📶 Triple play services
- 📶 Establishing a powerful wireless network

Key Features

The NetComm NL1901ACV enhanced VDSL2/ADSL2+/LTE hybrid wireless gateway providing an exceptionally fast and reliable broadband experience to your premises.

nbn and UFB ready

Featuring VDSL2/ADSL2 technologies as well as 4G LTE connectivity and a Gigabit WAN port, the NL1901ACV is an all-in-one triple play smart gateway that provides access to all nbn (National Broadband Network) and UFB (Ultra-Fast Broadband) fibre network configurations: **FTTC**, **FTTN**, **FTTB** and **FTTH**

Undisrupted connectivity

Benefit from hybrid technology to offer undisrupted broadband experience from the very start. Equipped with a 4G LTE category 4 module, the NL1901ACV hybrid gateway will connect to the mobile network to:

- 📶 **Offer Mobile fallback connectivity** - automatic switch to the 4G mobile network in case the fixed line service is disrupted and back, guaranteeing continuity of online operations during any downtime of your primary connection.
- 📶 **Connect sooner (Walk Out Working)** – the NL1901ACV enables superfast internet access before the fixed line service is even activated, allowing end users to connect faster, without waiting period!

Triple play services

The NL1901ACV is a triple play services enabler that supports the transmission of high-speed data, multi HD/UHD IPTV and over the top video streaming, VoIP feature for HD quality voice calls with the capacity to connect 2 phones.

Enhanced wireless experience

The NL1901ACV gateway embeds the 802.11 AC WiFi standard for powerful access point and HD video grade wireless capabilities. It allows both **2.4GHz** and **5GHz** bands to work concurrently, optimising performances and ensuring interoperability with all wireless equipment in the house or office.

Equipped with advanced 3 x 3 MIMO internal antennas, the NL1901ACV provides optimum reception while offering a strong signal throughout the home or business facilities.

Media sharing

Connect a **USB device** to the NL1901ACV gateway, access and share all A/V media and file content with all of the connected devices in the house in real time. The NL1901ACV becomes the media hub of the house using **DLNA/UPnP** standard and enhanced wireless capabilities to create a reliable high-speed home network.

The NL1901ACV has been designed to be placed on a desktop. All of the cables exit from the rear for easy organization. The display is visible on the front of the NL1901ACV to provide you with information about network activity and the device status.

Physical dimensions and weight

The table below lists the physical dimensions and weight of the NL1901ACV.

DIMENSIONS	
Width	230 mm
Height	200 mm
Depth	75 mm
Weight	562 grams (approx.)

Table 1 – Physical dimensions and weight table

NL1901ACV Default Settings

The following tables list the default settings for the NL1901ACV.

LAN (MANAGEMENT)	
Static IP Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1

Table 2 – LAN (Management) table

WIRELESS (WIFI)	
SSID	(Refer to the included Wireless Security Card)
Security	WPA2-PSK (AES)
Security Key	(Refer to the included Wireless Security Card)

Table 3 – Wireless (WIFI) table

NL1901ACV WEB INTERFACE ACCESS	
Username	admin
Password	The NL1901ACV's Serial Number

Table 4 – NL1901ACV WEB Interface Access table



Note – To replace the **Username** and **Password** with your personal choice go to: **Management > Access Control -- Passwords**

Your new username or password can be up to 16 characters or numbers and cannot contain spaces.

Enter the current **Username** and **New Username**, the **Old Password** and **New Password** and re-enter the new password in the **Confirm Password** field and click **Apply/Save** to apply the new settings.

Interfaces

The NL1901ACV has been designed to be placed on a desktop resting on its round pedestal.

User interface elements are found on the front, back and left side (viewed from the front) of the gateway device.

Front

The front of the NL1901ACV has a row of icons with LED lights behind them that provide information about the NL1901ACV's current status and network activity.



Figure 1 – NL1901ACV gateway front view






LED indicators

The colour and activity of the LED lights behind the icons indicate current status or activity of the functionality represented by each icon or number.



LED indicators on front of NL1901ACV

The following table explains the meaning of the LED indicator light displays.

LED INDICATOR	ICON	COLOUR / ACTIVITY	DEFINITION
Power		Red	After the NL1901ACV is powered on while it is initialising (normally 1-2 minutes).
		Green	The NL1901ACV is powered on and operating normally.
		Off	The power is off.
DSL		Off	No DSL signal detected.
		Green Blinking	Synching.
		Green	DSL synchronized.
Internet		Green	The NL1901ACV is connected to an internet service.
		Green Blinking	Data is being transmitted to or from the internet.
		Red	User ID/Password is configured wrong for DSL interface.
		Off	The NL1901ACV is not connected to the internet.
WAN		Green	A device is connected to the Ethernet WAN port.
		Green Blinking	Data is being transmitted to or from the WAN.
		Off	No device is connected to the Ethernet WAN port.
Ethernet	1 2 3 4	Green	A device is connected to the Ethernet LAN port.
		Green Blinking	Data is being transmitted to or from the Ethernet LAN port.
		Off	No device is connected to the Ethernet LAN port.
		Off	No device is connected to the Ethernet LAN port.
WiFi	2.4	Green	2.4G WiFi service is enabled.
		Green Blinking	Data is being transmitted to or from the Wireless interface.
		Off	WiFi is disabled.
	5	Green	5G WiFi service is enabled.
		Green Blinking	Data is being transmitted to or from the Wireless interface.
		Off	WiFi is disabled.
WPS		Green	WPS client is paired.
		Green Blinking	WPS pairing is triggered.
		Off	WPS is disabled.
USB	1 2	Green	A USB device is connected.
		Green Blinking	Data is being transmitted through the USB interface.
		Off	No USB device is connected to the USB interface.
Telephone		Green	A VoIP account is registered.



LED INDICATOR	ICON	COLOUR / ACTIVITY	DEFINITION
	1	Green Blinking	Incoming call or the handset is in use.
	2	Off	No handset registered
LTE		Off	No LTE connection.
		Green	LTE connection established.
LTE signal		Off	No LTE signal detected.
		1 Green	The LTE signal is weak.
		2 Green	The LTE signal is medium.
		3 Green	The LTE signal is strong.

Table 5 – LED indicator table

Rear

All of the cables attach from the rear together with the two antenna sockets.



Figure 2 – NL1901ACV gateway rear view

NO.	INTERFACE	DESCRIPTION
1	4G/LTE antennae sockets	For use with the SIM/LTE 4G functionality.
2	DSL	Use the provided RJ11 cable to connect the gateway to the telephone line operating your xDSL service.

NO.	INTERFACE	DESCRIPTION
3	Telephone 1 and 2	Connect a regular analogue telephone handset here for use with a VoIP service.
4	Ethernet 1 - 4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
5	WAN	Gigabit capable WAN port for connection to a WAN network. Connect to your Network Termination Device (NTD) for high-speed internet access.
6	Reset button	Reset unit to Default by inserting a thin metal wire into the hole and holding the Reset button down for 10 seconds when unit is powered on.
7	USB	Connect an external USB storage device here to use the Network Attached Storage (NAS) feature of the NL1901ACV.
8	2.4G WPS button	Press the 2.4G WPS button to activate the WPS PBC pairing function for the 2.4GHz radio.
9	5G WPS button	Press the 5G WPS button to activate the WPS PBC pairing function for the 5GHz radio.
10	USB 1 socket	Connect an external USB storage device here to use the Network Attached Storage (NAS) feature of the NL1901ACV.
11	Power supply jack	Connection point for the included power adapter. Connect the power supply here.

Table 6 – Rear interface table

Left Side







Figure 3 – NL1901ACV gateway side view

NO	INTERFACE	DESCRIPTION
1	SIM Card slot	Slot for 2FF form SIM card.
2	USB 2 socket	Connect an external USB storage device here to use the Network Attached Storage (NAS) feature of the NL1901ACV.
3	On/Off button	Toggles the power on and off.

Table 7 – Side interface table

Safety and product care

Your gateway is an electronic device that sends and receives radio signals. Please take the time to read this list of precautions that should be taken when installing and using the gateway.

-  Do not disassemble the gateway. There are no user-serviceable parts.
-  Do not allow the gateway to come into contact with liquid or moisture at any time. To clean the device, wipe it with a damp cloth.
-  Do not restrict airflow around the device. This can lead to the device overheating.
-  Do not place the device in direct sunlight or in hot areas.

Transport and handling

When transporting the NL1901ACV, it is recommended to return the product in the original packaging. This ensures that the product will not be damaged.



Attention – In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.

Installation and configuration of the NL1901ACV

Placement of your NL1901ACV



The wireless connection between your NL1901ACV and your WiFi devices will be strong when they are in close proximity and have direct line of sight. As your client device moves further away from the NL1901ACV or solid objects block direct line of sight to the gateway, your wireless connection and performance may degrade. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the NL1901ACV in order to see if distance is the problem.









Note – While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this check list may help

If you experience difficulties connecting wirelessly between your WiFi Devices and your NL1901ACV, please try the following steps:

-  In multi-storey homes, place the NL1901ACV on a floor that is as close to the centre of the home as possible. This may mean placing the NL1901ACV on an upper floor.
-  Try not to place the NL1901ACV near a cordless telephone that operates at the same radio frequency as the NL1901ACV (2.4GHz/5GHz).



Avoiding obstacles and interference



Avoid placing your NL1901ACV near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

-  Refrigerators
-  Washers and/or dryers
-  Metal cabinets
-  Large aquariums
-  Metallic-based, UV-tinted windows
-  If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal's path (between your devices and the NL1901ACV).

Cordless phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

-  Try moving cordless phones away from your NL1901ACV and your wireless-enabled computers.
-  Unplug and remove the battery from any cordless phone that operates on the 2.4GHz or 5GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the NL1901ACV.

-  If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your NL1901ACV to channel 11. See your phone's user manual for detailed instructions.
-  If necessary, consider switching to a 900MHz or 1800MHz cordless phone.

Choosing the “quietest” channel for your wireless network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Your wireless adapter may include a utility to assist in scanning for the least congested network, otherwise you may be able to find another piece of software that can be used. These tools display a graphical representation of the wireless networks in range and the channels on which they are operating. Try to find a channel which is not as busy and does not overlap with another one. Channels 1, 6 and 11 are the only channels on 2.4GHz which do not overlap with one another and you should ideally choose one of these channels. Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

Hardware installation

- 1 Connect the power adapter to the Power socket on the back of the NL1901ACV.
- 2 Plug the power adapter into the wall socket and switch on the power.
- 3 Wait approximately 60 seconds for the NL1901ACV to power up.

Connecting a client via Ethernet cable

- 1 Connect the yellow Ethernet cable provided to one of the yellow ports marked 'Ethernet' at the back of the NL1901ACV.
- 2 Connect the other end of the yellow Ethernet cable to your computer.
- 3 Wait approximately 30 seconds for the connection to establish.
- 4 Open your Web browser, and enter <http://192.168.20.1> into the address bar and press enter.
- 5 Follow the steps to set up your NL1901ACV.

Connecting a client wirelessly

- 1 Ensure WiFi is enabled on your device (e.g. computer/laptop/smartphone).
- 2 Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NL1901ACV.



Note – Refer to the included Wireless Security Card for the default SSID and wireless security key of your NL1901ACV.

- 3 When prompted for your wireless security settings, enter the Wireless security key configured on the NL1901ACV.
- 4 Wait approximately 30 seconds for the connection to establish.
- 5 Open your Web browser, and enter <http://192.168.20.1> into the address bar and press Enter.
- 6 Follow the steps to set up your NL1901ACV.

First-time setup wizard



Note – While we highly recommend that you set up your new gateway using the *First-time Setup Wizard (Basic Setup)*, it is possible to configure your new gateway directly from the [Advanced Setup](#) features.
It is also possible to initially set up your gateway using the Basic Setup wizard and then later fine-tune your configuration using the Advanced Setup tools.

Follow the steps below to configure your NL1901ACV Wireless gateway via its web based configuration wizard.

- 1 Open a web browser and type <http://192.168.20.1/> into the address bar at the top of the window.
- 2 At the login screen, type **admin** in the username and your NL1901ACV's serial number (located on the label pasted on the back of the device) into the password field, then click the **Login** button.



Note – 'admin' is the default username for the unit.
The gateway's serial number is the default password for the unit.
Both the username and password can be changed in **Management > Access Control > Passwords**

- 3 Click on the **Basic Setup** menu item on the left side of the screen.

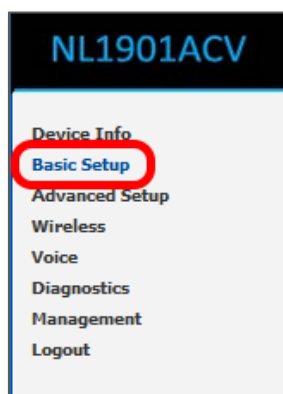


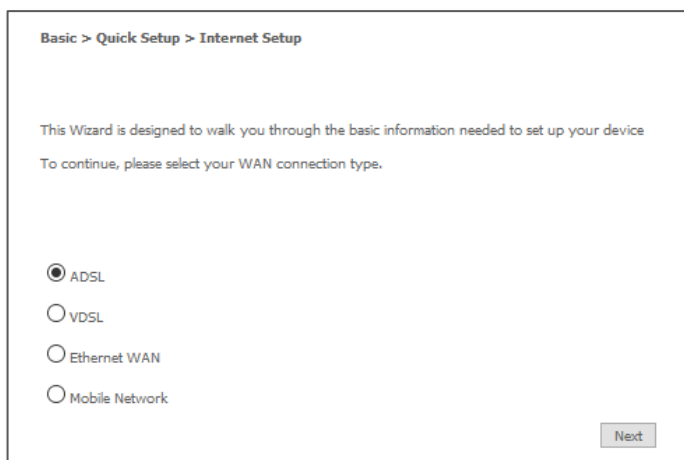
Figure 4 – NL1901ACV gateway – Select Basic Setup

Select WAN Connection Type

- 4 The first step is to define your data connection type.

Select ☒ the WAN connection type that you will be using.

- ☒ ADSL
- ☐ VDSL
- ☐ Ethernet WAN
- or
- ☐ Mobile Network



ADSL

ADSL, or Asymmetric digital subscriber line, is the most common internet connection for most residential settings. It allows high speed internet connections over copper telephone wires.

Your ISP will advise you of the service type and usually it will be ADSL.

The following diagram shows a typical ADSL setup, notice that it includes an optional phone handset.

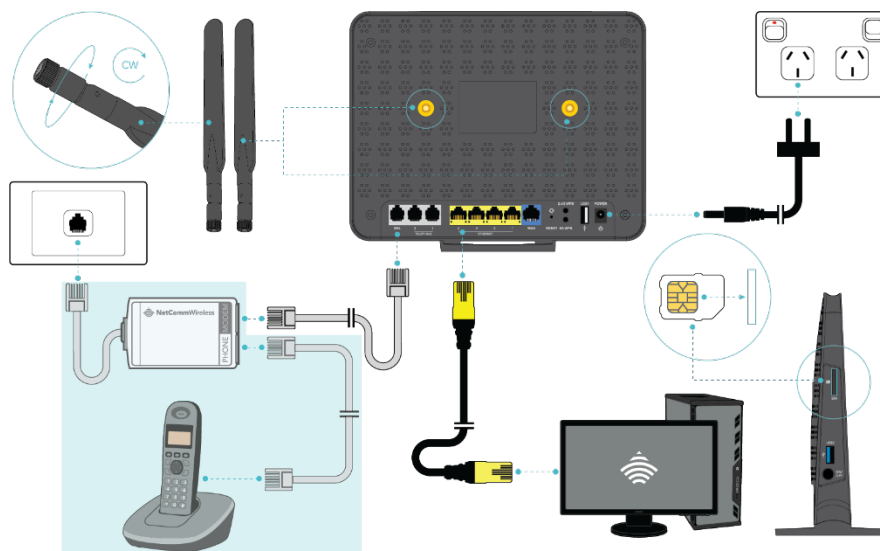


Figure 5 – NL1901ACV gateway – Common ADSL setup



Note – The **SIM** card pictured above is also optional. It can be deployed as the primary data connection or, more commonly, as a fallback protection in case the primary data connection fails. Refer to the **Mobile Network** section on page 30.

- a Select **ADSL** and click the **Next** button.

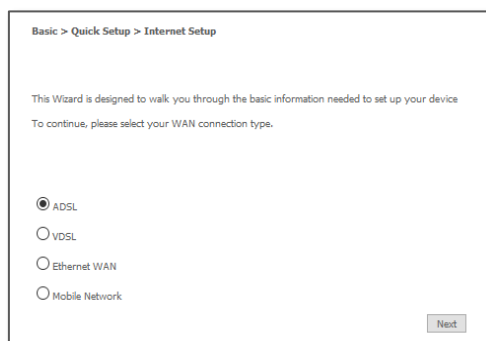


Figure 6 – NL1901ACV gateway – Select ADSL as WAN connection type

- b Select either the **PPPoE**, **PPPoA** or **Bridging** for your internet connection as specified by your Internet Service Provider (ISP).

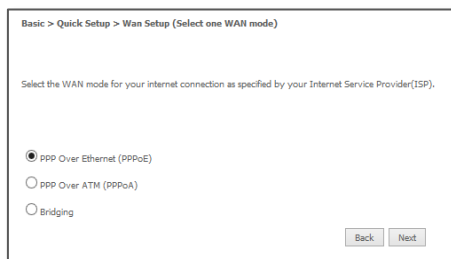


Figure 7 – Select PPPoE as WAN mode

- c Click the **Next** button.
- d In the **User ID** and **Password** fields, enter the PPPoE or PPPoA authentication username and password assigned to you by your Internet Service Provider (ISP). Bridging does not require a username or password.

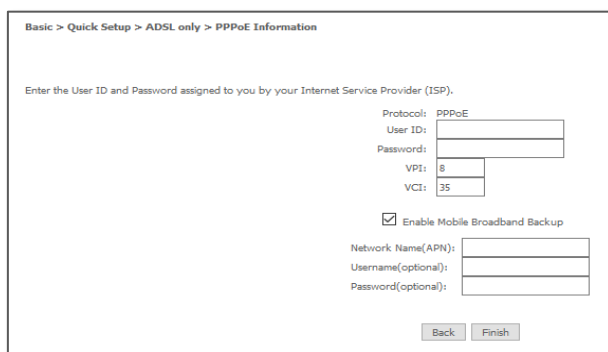


Figure 8 – Enter PPPoE User ID and Password

- e If you plan to use a SIM card for fallback protection via a mobile network connection, select ☒ **Enable Mobile Broadband Backup** and enter the **Network Name (APN)** and the **Username** and **Password**, if required. For more information on setting up fallback protection and unlocking the SIM, refer to the **Mobile Network** section on page 30.
- f Click the **Finish** button.
- g The account settings are saved and the NL1901ACV connects to the internet.

VDSL

VDSL, or Very-high-bit-rate digital subscriber line, also operates over copper telephone lines while offering faster data transmission than ADSL services, particularly in the upstream direction. It is a better solution for users who deliver large amounts of data as well as receiving data as downstream and upstream data transmission rates are roughly equal. ADSL gives priority to downstream data flow as most residential customers receive more data than they send. Not all ISPs offer VDSL services.

The following diagram shows a typical VDSL setup.

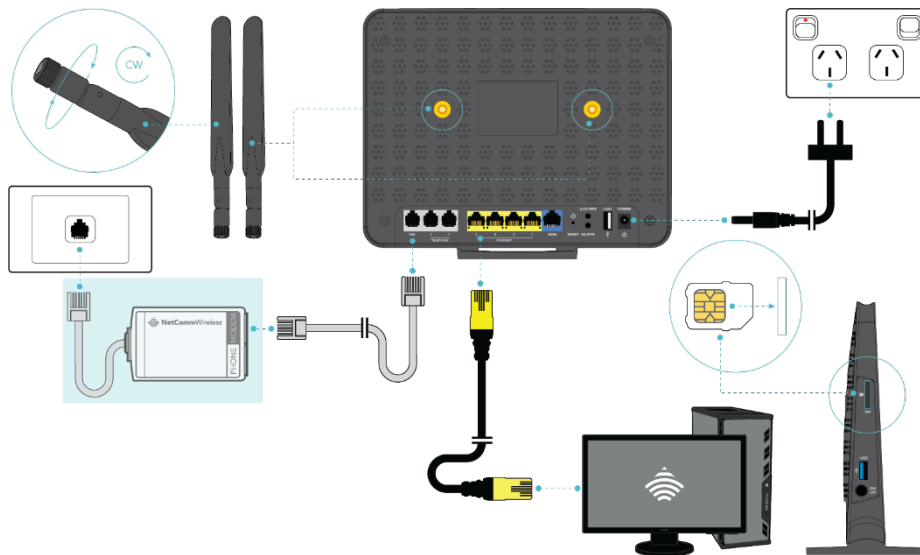


Figure 9 – NL1901ACV gateway – Common VDSL setup



Note – The **SIM** card pictured above is optional. It can be deployed as the primary data connection or, more commonly, as a fallback protection in case the primary data connection fails. Refer to the **Mobile Network** section on page 30.

- a Select ☒ **VDSL** and click the **Next** button.

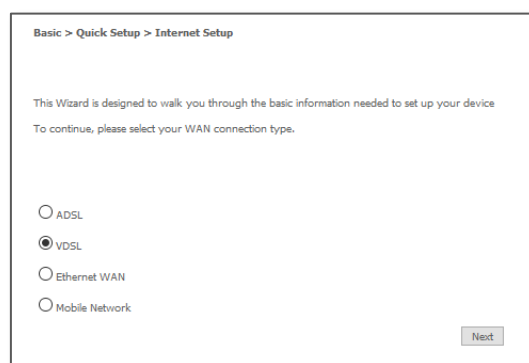


Figure 10 – NL1901ACV gateway – Select VDSL as WAN connection type

- b Select the WAN mode for your internet connection as specified by your Internet Service Provider (ISP).

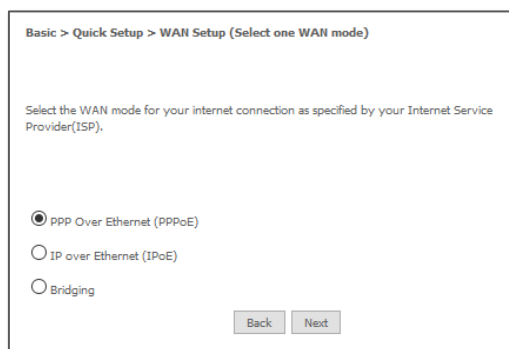


Figure 11 – Select WAN mode for VDSL connection

Click the **Next** button.

- c Select the correct VLAN option for your connection.

For New Zealand customers, the requirement for VDSL is **VLAN tag 10**.

If you are not sure of the tagging requirement for your connection, please contact your ISP.

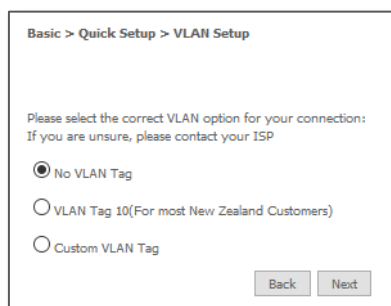


Figure 12 – Select VLAN option for VDSL connection

Click the **Next** button.

- d In the **User ID** and **Password** fields, enter the username and password assigned to you by your Internet Service Provider (ISP).

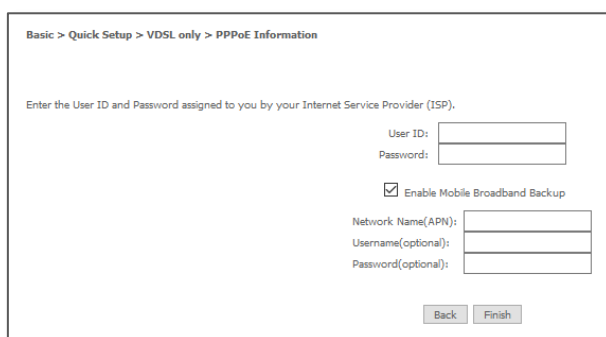


Figure 13 – VDSL connection – Enter PPPoE User ID and Password

- e If you plan to use a SIM card for fallback protection via a mobile network connection, select ☒ **Enable Mobile Broadband Backup** and enter the **Network Name (APN)** and the **Username** and **Password**, if required. For more information on setting up fallback protection and unlocking the SIM, refer to the **Mobile Network** section on page 30.



Note – If you select ☐ **Bridging** mode the ☐ **Enable Mobile Broadband Backup** (SIM card fallback protection) option is not available.

- f Click the **Finish** button when you have entered the required details.
The account settings are saved and the NL1901ACV connects to the internet.

Ethernet WAN

Select **Ethernet WAN** if you connect to the internet via an upstream gateway device such as an FTTP gateway or HFC cable gateway.

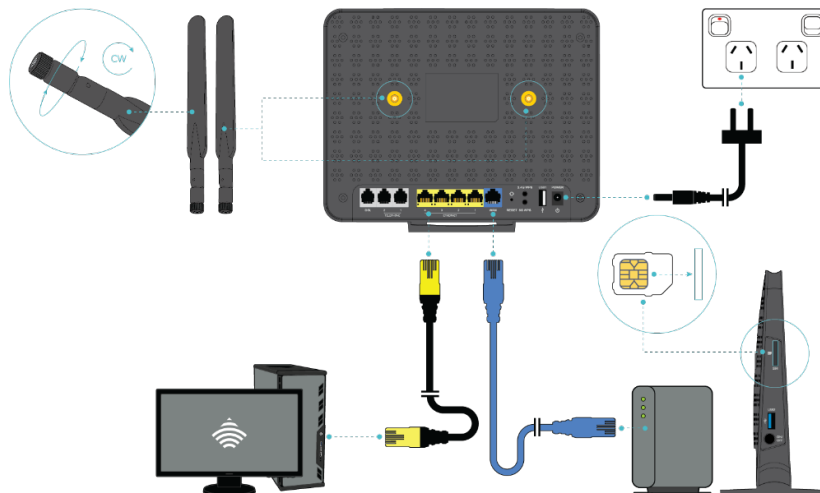


Figure 14 – NL1901ACV gateway – Ethernet WAN connection setup



Note – The **SIM** card pictured above is optional. It can be deployed as the primary data connection or, more commonly, as a fallback protection in case the primary data connection fails.
Refer to the **Mobile Network** section on page 30.

- Connect an RJ45 Ethernet cable to the **WAN** port on the NL1901ACV. Connect the other end of the cable to your WAN service.
- Select ☒ **Ethernet WAN** then click the **Next** button.

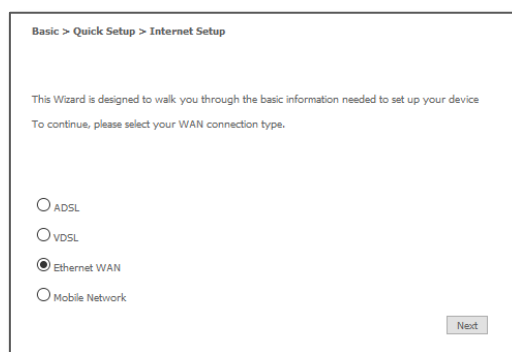


Figure 15 – NL1901ACV gateway – Select Ethernet WAN as WAN connection type

- c Select the WAN mode for your internet connection as specified by your Internet Service Provider (ISP).

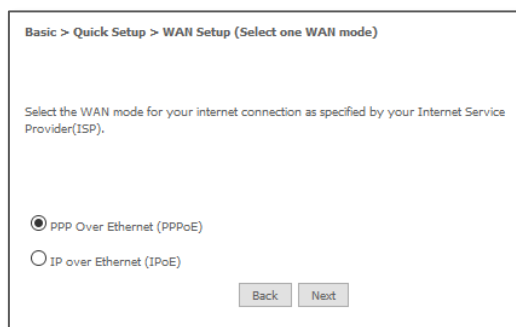


Figure 16 – Select WAN mode for Ethernet WAN connection

- d Click the **Next** button.

PPP over Ethernet (PPPoE)

If at step c you selected **PPP over Ethernet (PPPoE)**:

- i Select the correct VLAN option for your connection.
For **New Zealand** customers, the requirement for VDSL is **VLAN tag 10**.
If you are not sure of the tagging requirement for your connection, please contact your ISP.

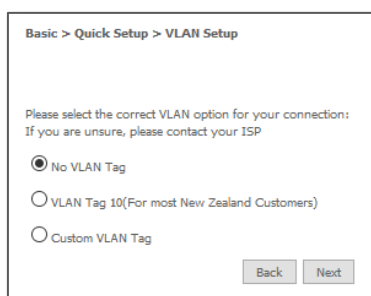


Figure 17 – Select VLAN option for PPPoE

- ii Click the **Next** button.
- iii Enter the User ID and Password assigned to you by your Internet Service Provider (ISP)
- iv If you want to set up the optional **Mobile Broadband** fallback facility, select ☒ **Enable Mobile Broadband Backup** and enter the following mobile network's details: **Network Name (APN)** and the **Username** and **Password**, if required. For more information on setting up fallback protection and unlocking the SIM, refer to the **Mobile Network** section on page 30.

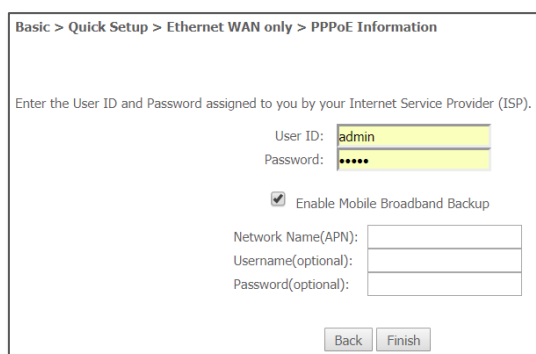


Figure 18 – Ethernet WAN connection – Enter User ID and Password

- v Click **Finish** to view the setup **Summary**.

IP over Ethernet (IPoE)

If at step c you selected **IP over Ethernet (IPoE)**:

- i Select the correct VLAN option for your connection. For **New Zealand** customers, the requirement for VDSL is **VLAN tag 10**. If you are not sure of the tagging requirement for your connection, please contact your ISP. Click the **Next** button.

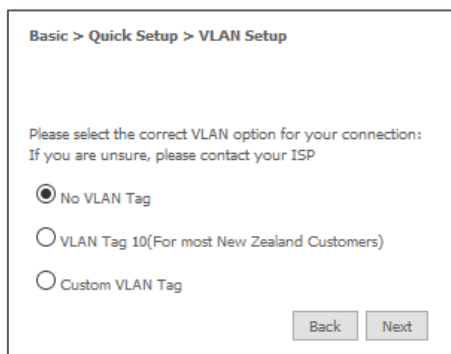


Figure 19 – IP over Ethernet (IPoE) – VLAN Setup

- ii If your ISP has supplied a static IP address, select **Use the following Static IP address** and enter the details, otherwise select **Obtain an IP address automatically**.

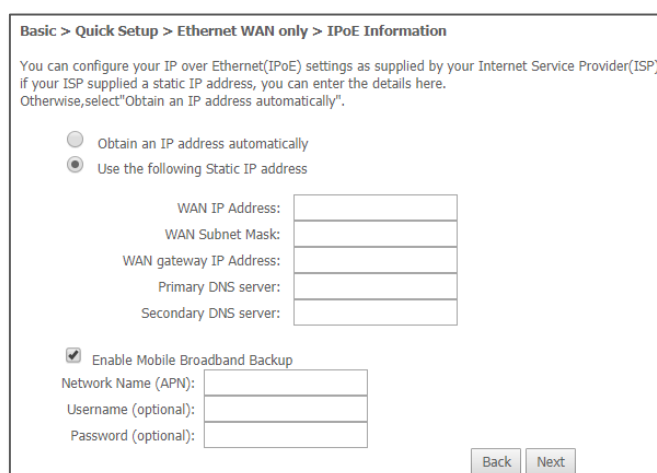




Figure 20 – IP over Ethernet (IPoE) – Static or Auto IP Address

- iii If you want to set up the optional **Mobile Broadband** fallback facility, select ☒ **Enable Mobile Broadband Backup** and enter the following mobile network's details: **Network Name (APN)** and the **Username** and **Password**, if required. For more information on setting up fallback protection and unlocking the SIM, refer to the **Mobile Network** section on page 30.
- iv Click the **Next** button to display details of the settings in a **Summary** page.
- v Click **Apply/Save** to activate the NL1901ACV's connection to the internet.

Mobile Network

There are two principle objectives reasons for using the SIM functionality:

-  Establish and use a **Mobile Network** as your sole data connection supplying internet access via a mobile broadband service. Depending on your mobile service, this option is potentially very expensive.
Or alternatively,
-  Set up a mobile network data connection as an optional fallback connection that will take over if the primary data connection (ADSL, VDSL or Ethernet WAN) connection fails. In this case, when you set up your primary data connection at the **PPoE/IPoE Information** stage of the Quick Setup process you must select ☒ **Enable Mobile Broadband Backup** and enter the mobile network's details.



Note – The **SIM** card must be in the 2FF format.

Prerequisites

To use the mobile network as the primary WAN connection, ensure that you have an active SIM card inserted into the gateway and that you have attached the two 4G/LTE antennas to the back of the gateway.

If you do not have an SIM card inserted, power off the gateway, insert the SIM card, then power it on again.

Attach the antennas by turning them in a clockwise direction in the antenna sockets.

Unlock SIM

When inserting a new SIM, it will have to be unlocked using its PIN.

SIMs in the gateway may from time to time become locked. Check on the **Device Info – Summary** page whether the **Device Info for Cellular network** displays **PIN locked** in the **SIM info** field.

If locked, unlock the SIM card going to **Advanced Setup > Mobile Broadband** and click the **Pin Manage** button.

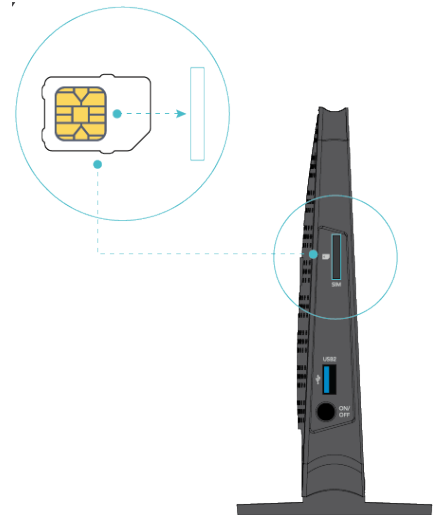
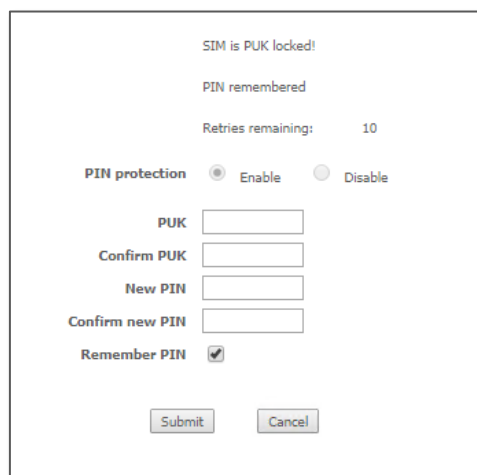



Figure 21 – Unlock PIN code – enter code

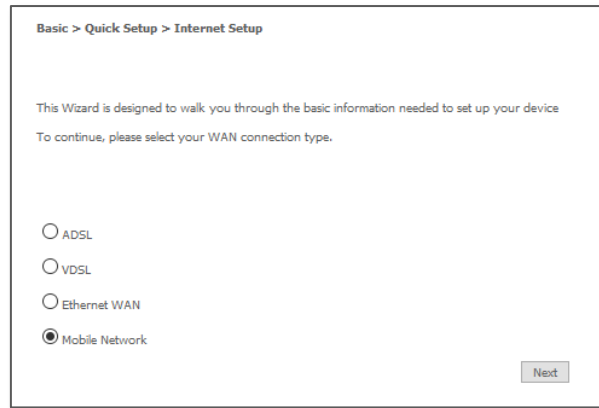
- i On the **USB mobile PIN Configuration** page the SIM card's status will be: **NEED PIN CODE!**
- ii Select ☒ **Unlock with PIN code** (if it is not already selected)
- iii Type in your four numeral code into the **Enter PIN code** field
- iv Click the **Submit** button.

- v In a few minutes the following confirmation will be displayed.

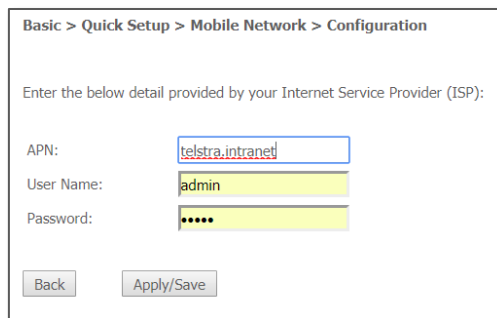
SIM card's Operation status is: **OK**

Setup Mobile Network

- i Click on **Basic Setup**, then select **Mobile Network**.



- ii Click the **Next** button.
- iii Enter the **APN** assigned by your carrier and, if required, enter a **username** and **password**.



- iv Click the **Apply/Save** button to activate the NL1901ACV's connection to the internet.

Device Info

Summary

When you log in to the gateway, the **Device Info** summary page is displayed, giving a general overview of the status of the gateway and the WAN connection.

Device Info

Device Info	
Manufacturer:	NetComm Wireless
Product Class:	NL1901ACV
Serial Number:	021018081710
Build Timestamp:	180822_2145
Software Version:	NL1901ACV.NC.AU-R6B014.EN
Bootloader (CFE) Version:	1.0.38-118.3
DSL PHY and Driver Version:	A2pv6F039v.d26r
VDSL PROFILE:	No profile
Wireless Driver Version:	7.35.260.64013
Voice Service Version:	Voice
Uptime:	3D 19H 16M 21S

Figure 22 – NL1901ACV gateway – Device Info section

ITEM	DEFINITION
Manufacturer	Indicates that NetComm is the manufacturer of this product.
Product Class	The model of the product.
Serial Number	The unique set of numbers assigned to the gateways for identification purposes.
Build Timestamp	The date and time that the software running on the gateway was published.
Software Version	The current firmware version installed on the gateway.
Bootloader (CFE) Version	The current boot loader version installed on the gateway.
DSL PHY and Driver Version	The driver version of the on-board DSL chip installed on the gateway.
VDSL PROFILE	The VDSL profile in use. Supports 8a, 8b, 12a and 17a VDSL profiles.
Wireless Driver Version	The current wireless driver installed on the gateway.
Voice Service Version	The driver version of the chip set.
Uptime	The number of days, hours and minutes that the gateway has been running.

Table 8 – Device Info details table

WAN Connection Status

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.20.1
Service connection type:	mobile
Default Gateway:	10.100.245.28
Primary DNS Server:	10.4.58.204
Secondary DNS Server:	10.5.136.242
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	
Date/Time:	Tue Oct 2 10:28:04 2018

Figure 23 – NL1901ACV gateway – WAN connection status section

ITEM	DEFINITION
Line Rate – Upstream (Kbps)	The current synchronisation upstream speed of the DSL connection in Kbps (Kilobits per second).
Line Rate – Downstream (Kbps)	The current synchronisation downstream speed of the DSL connection in Kbps (Kilobits per second).
LAN IPv4 Address	The current IPv4 LAN IP address assigned to the gateway.
Service connection type	Displays whether the WAN connection is ADSL/VDSL or Ethernet WAN.
Default Gateway	The current default gateway address of the WAN interface.
Primary DNS Server	The current primary DNS server in use
Secondary DNS Server	The current secondary DNS server is use.
LAN IPv6 ULA Address	The current IPv6 LAN IP address in use if assigned.
Default IPv6 Gateway	The current IPv6 default gateway if assigned.
Date/Time	The current local date and time set on the gateway.

Table 9 – WAN connection details table

Cellular Network Connection Status

If you have enabled a SIM and are using it either as your primary data source via a **Mobile Network** broadband service or as a fallback connection providing redundancy should your primary ADSL/VDSL/Ethernet WAN be interrupted, this table will show the device status when this LTE service is being used.


Device Info for Cellular network	
Network:	Telstra Mobile Telstra
Network selection mode:	Automatic
APN:	telstra.internet
Link:	Connected
Service Type:	Auto
Signal Strength:	
SIM info:	SIM inserted
Connection Up Time:	03 day: 17 hr: 32 min: 35 sec

Figure 24 – NL1901ACV gateway – Cellular Network connection status section

ITEM	DEFINITION
Network	The network operator that supplies the cellular service.
Network selection mode	Can be set exclusively for 3G or LTE (4G) , or Auto which selects 4G first and then 3G if 4G not available.
APN	The Access Provider Name used by network operator.
Link	The current status of the cellular connection: Connected , Not connected , etc.
Service Type	Type of mobile connection established: 3G or LTE
Signal Strength	Five levels of signal strength appear in the bar icons. If all bars are empty, no signal is detected or there is no connection. The bars will fill with colour progressively from the left as the signal strength improves. Note – If an enabled SIM is inserted, signal strength will be detected, measured and indicated regardless of whether a connection to a network operator exists or not.
SIM info	Indicates whether a valid SIM card is inserted into the SIM socket or not. Note – Unit must first be turned off before inserting SIM card for it to be detected on startup.
Connection Up Time	The time (in days, hours, minutes and seconds) since the cellular connection was last established.

Table 10 – Cellular Network connection details table

WAN

The **WAN** page shows more detailed information related to the WAN interface configuration, including the firewall status, IPv4 and IPv6 addresses of the gateway.

WAN Info													
Interface	Description	Type	VLAN Mux ID	IPv6	IGMP Pxy	IGMP Source Enable	MLD Pxy	MLD Source Enable	NAT	Firewall	Status	IPv4 Address	IPv6 Address
eth4.1	ETH WAN	IPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	Unconfigured	0.0.0.0	
lte0	mobile		Disabled	Disabled	Disabled	Disabled			Enabled	Enabled	Connected	10.100.239.10	
ppp0.1	VDSL	PPPoE	Disabled	Disabled	Disabled	Disabled			Enabled	Enabled	Unconfigured	0.0.0.0	

Figure 25 – NL1901ACV gateway – WAN Info list

ITEM	DEFINITION
Interface	The Interface of the WAN connection.
Description	The description of the WAN connection.
Type	The type of WAN connection.
VLAN Mux ID	Details the status of VLAN Mux ID, if used.
IPv6	The status of IPv6.
IGMP Pxy	Details the status of IGMP (Internet Group Management Protocol) traffic on each WAN connection. IGMP is only used with IPv4 connections. IGMP proxy enables the gateway to issue IGMP host messages on behalf of hosts that the gateway discovered through standard IGMP interfaces, allowing NAT transversal of Multicast traffic.
IGMP Source Enable	Details the status of IGMP source on each WAN connection. IGMP Sources function send a membership report that includes a list of IGMP source addresses.
MLD Pxy	Shows the status of the Multicast Listener Discovery protocol when IPv6 is in use. Multicast Listener Discovery (MLD) proxy enables the gateway to issue MLD host messages on behalf of hosts that the gateway discovered through standard MLD interfaces.
MLD Source Enable	Details the status of MLD source on each WAN connection. MLD Sources function can send a membership report that includes a list of MLD source addresses.
NAT	The NAT (Network Address Translation) status of the WAN connection: Enabled or Disabled
Firewall	The status of the gateway firewall across the WAN connection.
Status	The status of the WAN connection: Connected , Unconfigured , etc.
IPv4 Address	The current IPv4 address of the WAN interface.
IPv6 Address	The current IPv6 address of the WAN interface.

Table 11 – WAN Info table

Statistics

Statistics – LAN

The **Statistics – LAN** page shows detailed information about the number of bytes, packets, errors and dropped packets on each LAN interface in both directions of communication.

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
eth0	742666	7173	0	1	0	1011	5512	650	7615128	7688	0	0	0	333	7342	13
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0	0	0	0	28	0	0	0	0	377791	4174	0	0	0	0	0	0
wl0.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl1	0	0	0	39	0	0	0	0	0	0	0	0	0	0	0	1
wl1.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl1.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl1.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

Figure 26 – Device Info – Statistics – LAN display

INTERFACE	DESCRIPTION	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.
	Packets	Rx/Tx (receive/transmit) packets.
	Errors	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Table 12 – Statistics – LAN display table

Statistics – WAN Service

The **Statistics – WAN Service** page shows detailed information about the number of bytes, packets, errors and dropped packets on the WAN interface in both directions of communication.

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
ppp0.1	VDSL	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth4.1	ETH WAN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
lte0	mobile	475397	3507	0	0	0	0	0	0	279118	3699	0	0	0	0	0	0

Reset Statistics

Figure 27 – Device Info – Statistics – WAN Service display

INTERFACE	DESCRIPTION	
Interface	The type of interface for each connection.	
Description	A description of the connection type.	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.
	Packets	Rx/Tx (receive/transmit) packets.
	Errors	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Table 13 – Statistics – WAN Service table

Statistics – xTM

The **Statistics – xTM** page shows details related to the xTM (ATM/PTM) interface of the gateway.

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
-------------	-----------	------------	------------	-------------	--------------	---------------	--------------	---------------	------------------	----------------

Figure 28 – Device Info – Statistics – xTM display

INTERFACE	DESCRIPTION
Port Number	The port number used by the xTM interface.
In Octets	The number of data packets in octets received over the ATM interface.
Out Octets	The number of data packets in octets transmitted over the ATM interface.
In Packets	The number of data packets received over the ATM interface.
Out Packets	The number of data packets transmitted over the ATM interface.
In OAM Cells	Operation, Administration, and Maintenance (OAM) Cell is the ATM Forum specification for cells used to monitor virtual circuits.
Out OAM Cells	Operation, Administration, and Maintenance (OAM) Cell is the ATM Forum specification for cells used to monitor virtual circuits.
In ASM Cells	The number of Any Source Multicast (ASM) cells received over the interface.
Out ASM Cells	The number of Any Source Multicast (ASM) cells transmitted over the interface.
In Packets Errors	The number of packets with errors detected over the xTM interface.
In Cell Errors	The number of cells with errors detected over the xTM interface.

Table 14 – Statistics – xTM settings table

Statistics – xDSL

The Statistics – xDSL page shows details related to the DSL interface of the gateway.

Statistics -- xDSL

Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test
Reset Statistics

Figure 29 – NL1901ACV gateway

Bit Error Rate (BER) test

Click the **xDSL BER Test** button to run a bit error test. The test determines the quality of the ADSL connection by transferring and receiving data containing a known patterns and checking the sent and received data for any errors.

ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec):

Start Close

ADSL BER Test – Select time

xDSL BER Test - Running

The xDSL BER test is in progress. The connection speed is 0 Kbps.

The test will run for seconds.

Click "Stop" to terminate the test.

Stop Close

ADSL BER Test – Run test

xDSL BER Test - Result

The xDSL BER test completed successfully.

Test Time (sec):	
Total Transferred Bits:	
Total Error Bits:	
Error Ratio:	

Close

ADSL BER Test – Test Results

Route

The **Route** page displays any routes that the gateway has created.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	10.102.141.113	0.0.0.0	UG	0	mobile	lte0
10.4.27.70	10.102.141.113	255.255.255.255	UGH	64	mobile	lte0
10.5.133.45	10.102.141.113	255.255.255.255	UGH	64	mobile	lte0
10.102.141.112	0.0.0.0	255.255.255.252	U	0	mobile	lte0
192.168.20.0	0.0.0.0	255.255.255.0	U	0		br0

Figure 30 – Device Info -- Route list

ARP

Click **ARP** to display the address resolution protocol information.

This option can be used to determine which IP address / MAC address is assigned to a particular host. This can be useful when setting up URL filtering, Time of Day filtering or Static DHCP addressing.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.20.2	Complete	2c:44:fd:12:3c:6e	br0

Figure 31 – Device Info -- ARP list

DHCP

Click **DHCP** to display the Dynamic Host Configuration Protocol (DHCP) lease information.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
NTCWKS0102	ec:08:6b:02:aa:0a	192.168.20.2	49710 days, 6 hours, 28 minutes, 15 seconds

Figure 32 – Device Info -- DHCP Leases list

You can use this to determine when a specific DHCP lease will expire, or to assist you with setting up Static DHCP addressing.

CPU & Memory

The CPU & Memory page shows real-time graphs charting the physical memory usage and the work load of the CPU.

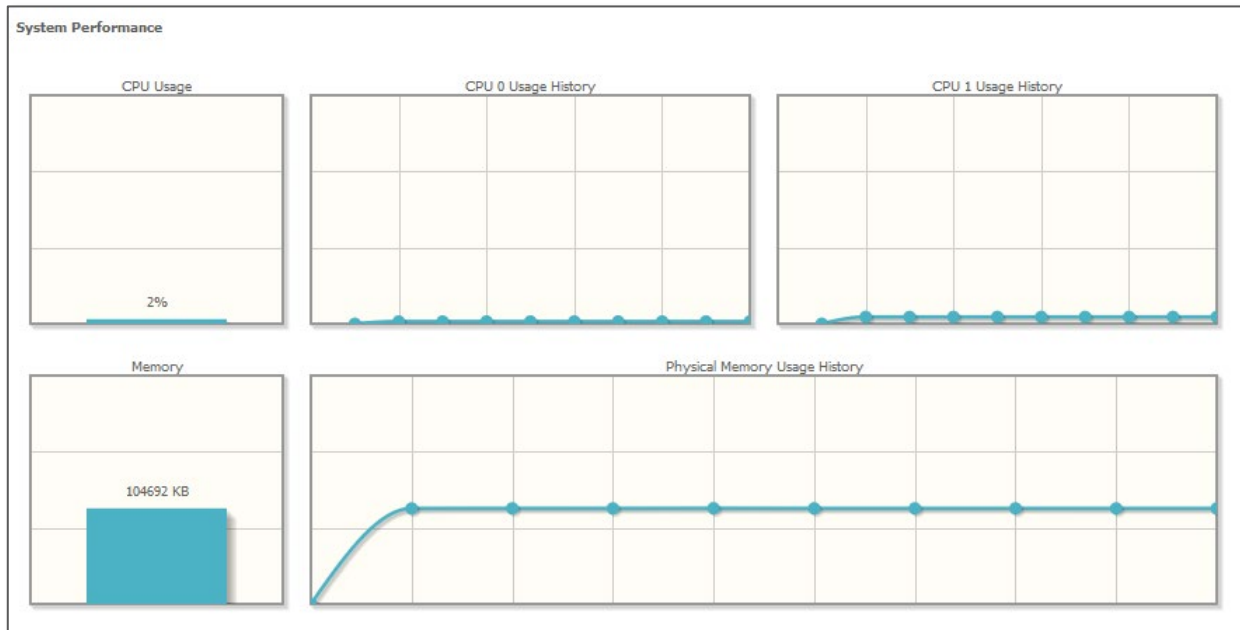


Figure 33 – Device Info – CPU & Memory display

Advanced Setup

While you can set up your gateway directly from the **Advanced Setup** pages, we recommend that you use the *First-time Setup Wizard* contained in the [Basic Setup](#) section, see above.

Layer 2 Interface

ATM Interface

The ATM (Asynchronous Transfer Mode) interface page shows the settings of all available DSL ATM interfaces.

ATM interface is used for ADSL connections.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	VPI	VCI	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Min Cell Rate(cells/s)	Link Type	Connection Mode	IP QoS	MPAAL Precedence/Algorithm/Weight	Remove
ipoa0	8	35	Path0	UBR					IPoA	DefaultMode	Support	8/WRR/1	<input type="checkbox"/>

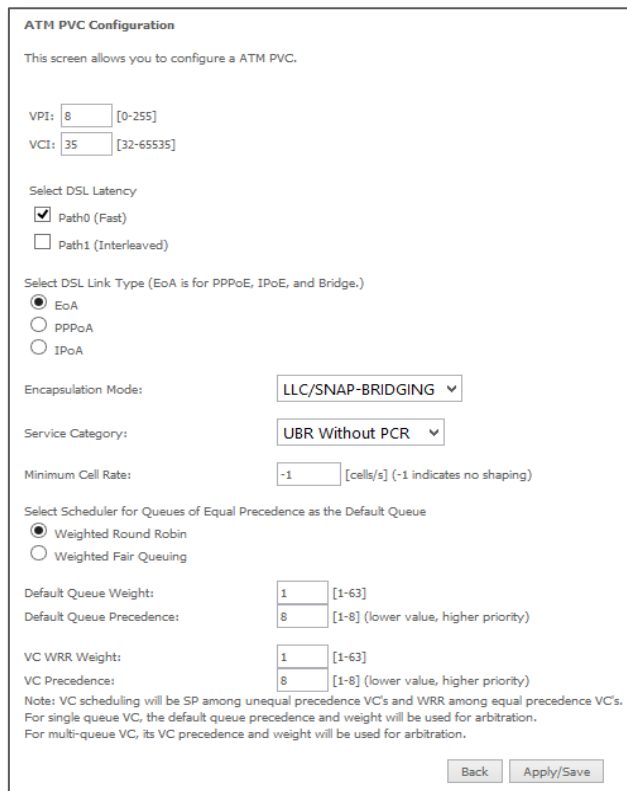
Figure 34 – DSL ATM Interface list

FIELD	DESCRIPTION
Interface	This field shows the interface name.
VPI	This field shows the Virtual Path Identifier (VPI) value. For most Australian connections the VPI is 8, for most New Zealand connections the VPI is 0. Refer to your ISP for the correct value.
VCI	This field shows the Virtual Channel Identifier (VCI) value. For most Australian connections the VCI is 35, for most New Zealand connections the VCI is 100. Refer to your ISP for the correct value.
DSL Latency	The value of the DSL Latency.
Category	This field shows the ATM service classes.
Peak Cell Rate (cell/s)	The maximum number of cells that may be transferred per second over the ATM interface.
Sustainable Cell Rate (cell/s)	An average, long-term cell transfer rate on the ATM interface.
Max Burst Size (bytes)	The maximum allowable burst size of cells that can be transmitted contiguously on the ATM interface.
Min Cell Rate (cell/s)	The minimum allowable rate at which cells may be transferred on the ATM interface.
Link Type	This field shows the type of link in use.
Connection Mode	This field shows the selected mode of connection.
IP QoS	This field shows the status of the Quality of Service (QoS) function.

FIELD	DESCRIPTION
MPAAL Prec/Alg/Wght	This displays data related to QoS Queue priority and algorithm.
Add button	Click to create a new ATM configuration.
Remove button	Check <input checked="" type="checkbox"/> the box in this field and click the Remove button to permanently delete an ATM configuration.

Table 15 – DSL ATM Interface Configuration settings table

To add an ATM interface, click the **Add** button. Enter the details as required by your Internet Service Provider and click the **Apply/Save** button.



ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: [0-255]
VCI: [32-65535]

Select DSL Latency
☒ Path0 (Fast)
☐ Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
☒ EoA
☐ PPPoA
☐ IPoA

Encapsulation Mode:

Service Category:

Minimum Cell Rate: [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue
☒ Weighted Round Robin
☐ Weighted Fair Queuing

Default Queue Weight: [1-63]
Default Queue Precedence: [1-8] (lower value, higher priority)

VC WRR Weight: [1-63]
VC Precedence: [1-8] (lower value, higher priority)

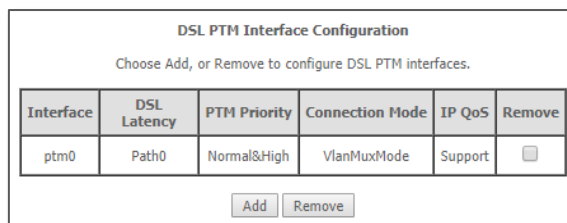
Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.
For single queue VC, the default queue precedence and weight will be used for arbitration.
For multi-queue VC, its VC precedence and weight will be used for arbitration.

Figure 35 – ATM PVC Configuration page

PTM Interface

The gateway can also establish DSL connections using PTM (Packet Transfer Mode). This page shows you an overview of the PTM interfaces and allows you to add or remove them.

PTM interface is used for VDSL connections.



DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	<input type="checkbox"/>

Figure 36 – DSL PTM Interface list

Click the **Add** button to create a new PTM interface.

Enter the details as required by your Internet Service Provider and click the **Apply/Save** button.

PTM Configuration

This screen allows you to configure a PTM connection.

Select DSL Latency

☒ Path0 (Fast)

☐ Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence

☒ Round Robin (weight=1)

☐ Weighted Fair Queuing

Default Queue Weight: [1-63]

Default Queue Precedence [1-8] (lower value, higher priority)

Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

Figure 37 – PTM Configuration page

ETH Interface

The ETH interface page allows you to add or remove ETH WAN interfaces.

ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Name	Connection Mode	Remove
eth4/eth4	VlanMuxMode	<input type="checkbox"/>

Figure 38 – ETH WAN interface list WAN Service



Note – When eth4 - ETH WAN Layer 2 interface is removed, the ETH WAN port will behave as an additional Ethernet LAN port.

WAN Service

The WAN Service page displays the current Wide Area Network service setup and allows you to configure the gateway to connect to a larger network for Internet access.



Attention – WAN service requires a preconfigured Layer 2 interface, be it ATM/PTM or Ethernet WAN.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	VLAN 802.1p	VLAN Mux ID	IGMP Proxy	IGMP Source	NAT	Firewall	IPv6	MLD Proxy	MLD Source	Remove	Edit	Action
eth4.1	ETH WAN	IPoE	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	
ppp0.1	VDSL	PPPoE	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="Connect"/>

Figure 39 – NL1901ACV gateway

To add a WAN service, click the **Add** button.

Use the drop down list to select the layer 2 interface to use for the WAN service and click the **Next** button.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

eth4/eth4

▼

Figure 40 – WAN Service – Select layer 2 interface

Select a WAN service type, enter a **Service Description**, enter the **802.1P Priority** and **802.1Q VLAN ID** if required, then click the **Next** button.

To disable VLAN tagging, place input value of -1. Refer to your ISP for VLAN information as required by your Internet Service Provider.

WAN Service Configuration

Select WAN service type:

☒ PPP over Ethernet (PPPoE)

☐ IP over Ethernet

☐ Bridging

☐ Allow as IGMP Multicast Source

☐ Allow as MLD Multicast Source

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

Figure 41 – WAN Service – Select WAN Service Type

PPP over Ethernet

Enter the PPPoE authentication details as required by your Internet Service Provider and click the **Next** button.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

MTU[576-1492]:

☒ Enable NAT

☐ Enable Fullcone NAT

☒ Enable Firewall

☐ Dial on demand (with idle timeout timer)

☐ PPP IP extension

☐ Use Static IPv4 Address

☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast Proxy

☐ Enable IGMP Multicast Proxy

☐ Enable IGMP Multicast Source

Figure 42 – Enter PPP over Ethernet details

IP over Ethernet

Enter the details as required by your Internet Service Provider and click the **Next** button.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
 If "Use the following Static IPv4/IPv6 address" is chosen, enter the WAN IPv4/IPv6 address, subnet mask/prefix Length and interface gateway.

☒ Obtain an IP address automatically

Option 55 Request List : (e.g:1,3,6,12)

Option 58 Renewal Time: (hour)

Option 59 Rebinding Time: (hour)

Option 60 Vendor ID: udhcp 0.9.9-pre

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 77 User ID:

Option 125: ☒ Disable ☐ Enable

☐ Use the following Static IP address

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Primary DNS server:

Secondary DNS server:

Figure 43 – Enter IP over Ethernet details

Select the **NAT Translation** settings as desired and click the **Next** button.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☒ Enable NAT

☐ Enable Fullcone NAT

☒ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast Proxy

☐ Enable IGMP Multicast Source

Figure 44 – Enter PPP over Ethernet NAT Translation settings

Bridging

When you select **Bridging** mode, a summary of the settings is displayed.

WAN Setup - Summary
 Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Figure 45 – WAN Setup - Bridging

Click **Apply/Save** to commit the settings.

Mobile Broadband

The **Mobile Broadband** page displays the current Wide Area Network service setup and allows you to configure the gateway to connect to a mobile (cellular) network for primary Internet access.

Only one **Mobile Broadband** can be set up at a time. You can alter the setup by clicking the **Edit** button, or **Remove** the setup and **Add** a new service.

Modem Status SIM CARD INVALID OR NO SIM CARD!

Wide Area Network (WAN) Service For Mobile Broadband Setup
 Choose Add, Remove or Edit to configure a WAN service For Mobile Broadband interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Manage	Edit	Action
lte0	mobile	mobile	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="button" value="PIN"/>	<input type="button" value="Edit"/>	<input type="button" value="Connect"/>

Figure 46 – NL1901ACV Mobile Broadband setup

FIELD	DESCRIPTION
Gateway status indicator	In the top left corner above the start of the table is the Gateway status indicator: diaalling... , CONNECTED , Manual Dialed , undialing... , DISCONNECT , SIM CARD INVALID OR NOT SIM CARD! , etc.
Interface	The interface of the mobile connection.
Description	The description of the mobile connection.
Type	The type of WAN connection.
Vlan802.1p	N/A for mobile interface.
VlanMuxId	N/A for mobile interface.

FIELD	DESCRIPTION
IGMP	Internet Group Management Protocol (IGMP) is used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
NAT	NAT (Network Address Translation) status of the mobile WAN connection: Enabled or Disabled
Firewall	The status of the gateway firewall across the mobile WAN connection.
IPv6	If IPv6 is available it can be Enabled , otherwise it will be Disabled .
MLD	Multicast Listener Discovery (MLD) is used by IPv6 routers for discovering multicast listeners.
Manage PIN button	Click to open the PIN settings page where you can enable, disable and change the PIN on the SIM.
Edit setup details button	Click open the Mobile Broadband Setup page to edit the details of the current Mobile Broadband connection.
Action: Connect/Disconnect button	Click the Connect button to manually connect to the Mobile broadband interface. When connected this button changes to Disconnect and allows the user to manually disconnect.
Add button	Click open the Mobile Broadband Setup page, see next section.
Remove setup button	You can only have one Mobile Broadband at a time. To add a replacement setup click Remove and then click Add .
Information button	Click to see details of the mobile broadband connection.

Table 16 – USB Mobile configuration settings table

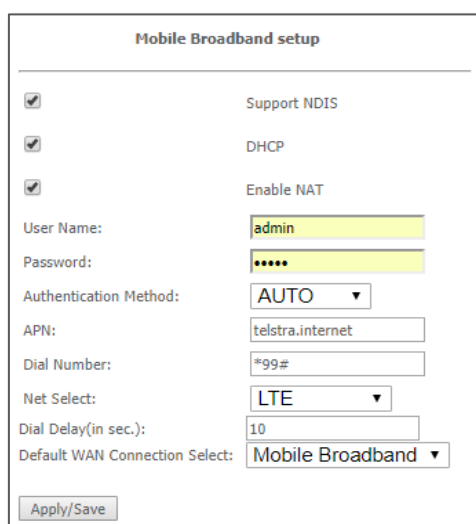
Add/Edit Mobile Broadband Setup

Only one mobile cellular service can be defined at one time.

If one is not currently defined, click the **Add** button.

If one already exists, either click the **Edit** button or click the **Remove** button and then click the **Add** button.

Both the **Add** and the **Edit** buttons open the **Mobile Broadband setup** dialog.



The image shows a screenshot of the 'Mobile Broadband setup' dialog box. It contains the following fields and options:

- ☒ Support NDIS
- ☒ DHCP
- ☒ Enable NAT
- User Name:
- Password:
- Authentication Method:
- APN:
- Dial Number:
- Net Select:
- Dial Delay(in sec.):
- Default WAN Connection Select:
-

Figure 47 – Mobile Broadband setup interface

FIELD	DESCRIPTION
Enable NAT	<input checked="" type="checkbox"/> Enable NAT (Network Address Translation) is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the router modifies network traffic sent and received to inform remote computers on the internet that packets originating from a machine behind the router originated from the WAN IP address of the router's internal NAT IP address. This may be disabled if a framed route configuration is required and local devices require WAN IP addresses
User Name	The Username for your broadband service provided by your broadband ISP.
Password	The Password for your broadband service provided by your broadband ISP.
Authentication method	Choose: AUTO, PAP, CHAP or MSCHAP
APN	Enter the APN (Access Point Name) provided by your broadband ISP.
Dial Number	Enter the number to dial to get data connectivity provided by your broadband ISP.
Net Select	Select the service your ISP provides, 3G or LTE or allow the router to auto-detect using AUTO .
Dial Delay (in secs.)	Enter the time delay in seconds that must elapse before re-connecting to the mobile connection when primary connection dropped, and mobile broadband is configured as backup.
Default WAN Connection Select	Select either Mobile Broadband or DSL OR ETHERNET .
WAN backup mechanism	DSL
	IP connectivity
Apply/Save button	Click to save and apply your changes.

Table 17 – DSL ATM Interface Configuration settings table



Note – Mobile Broadband service requires an unlocked SIM card in the 2FF format. See **PIN settings** section on the next page.

PIN settings

When **gateway status** DISCONNECT is displayed, click the **PIN** button in the **Manage** column to open the **PIN settings** page:

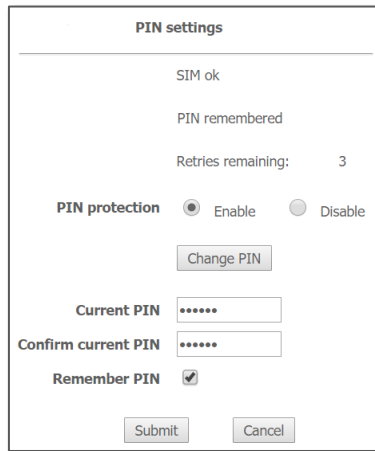


Figure 48 – SIM – PIN settings

The following fields are found on this page.

FIELD	DESCRIPTION
SIM card's Status	Current status of the SIM card.
PIN's Status	Current status of the SIM card's PIN.
PIN Retries remaining	Enter the number of tries allowed before the system PUK locks the SIM card. The default is three (3) attempts.
PIN protection	When <input checked="" type="radio"/> Enable is selected, the current PIN must be entered. When <input type="radio"/> Disable is selected, PIN entry not required.
Change PIN button	When PIN protection is <input checked="" type="radio"/> Enable click Change PIN to change the PIN to something easier to remember or more secure.
Current PIN	Shows the new or current PIN.
Confirm Current PIN	Re-enter the Current PIN .
Remember PIN	Select to allow your browser to retain the PIN in its memory.
Submit button	Click to save and apply the changes.
Cancel button	Click to close without saving and return to the broadband setup page.

Table 18 – USB mobile PIN Configuration page

IPv4 Autoconfig

The LAN window allows you to modify the settings for your local area network (LAN).



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. Group Name: **Default** ▼

IP Address:
 Subnet mask:

☒ Enable IGMP Snooping

☐ Standard Mode
☒ Blocking Mode

Enable IGMP LAN to LAN Multicast: **Disable** ▼
(LAN to LAN Multicast is effective only when exist route mode WAN service which is connected and enable igmp proxy.)

☐ Enable LAN side firewall

☐ Disable DHCP Server
☒ Enable DHCP Server

Start IP Address:
 End IP Address:
 Primary DNS server:
 Secondary DNS server:
 Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		

☐ Enable DHCP Server Relay
 DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

Figure 49 – LAN setup -- IPv4 Autoconfig settings

The following options are available to configure:

PARAMETER	DEFINITION
IP Address	Enter the Local IP Address to use for the NL1901ACV.
Subnet Mask	Enter the subnet mask to define the subnet of the Local Network.
Enable IGMP Snooping	Enable IGMP Snooping and select the IGMP Snooping mode to use. Standard: allow all multicast traffic to LAN clients. Blocking: only allow multicast subscribed clients to receive multicast packets.
Enable LAN side Firewall	Enable the LAN side firewall to restrict traffic between LAN host-LAN hosts and WiFi Clients.
Enable DHCP Server	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.

PARAMETER	DEFINITION
Enable DHCP Server Relay	Disabled DHCP server, and relay all request to external server specified by the IP address.
Configure the second IP Address	This option enables you to set a secondary IP Address for the NL1901ACV

Table 19 – IPv4 Autoconfig settings table

You can also reserve DHCP Addresses for specific hosts as shown below:



Figure 50 – Enter DHCP Static IP Addresses

To set a DHCP reservation, enter the MAC Address of the chosen host and IP to use and then click **Apply/Save**.

The NL1901ACV enables you to set the DHCP options which are provided to hosts attempting to connect to the DHCP server.

These options should not normally need to be set or changed. Click **Apply/Save** to save the new LAN configuration settings.

IPv6 Autoconfig

The IPv6 LAN Auto Configuration page allows you to configure settings pertaining to the IPv6 service.

IPv6 LAN Auto Configuration

Note:

1: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION '::'. Please enter the complete information. For example: Please enter '0:0:0:2' instead of '::2'.

2: Unique local address must start with "fd". The prefix and the address must be in same network and the prefix length must be 64.

☒ Enable ULA Prefix Advertisement
☒ Randomly Generate
☐ Statically Configure

Interface Address (prefix length is required): (e.g: fd80::/64)

Prefix:

Preferred Life Time (hour):

Valid Life Time (hour):

IPv6 LAN Applications

☐ Enable DHCPv6 Server
☒ Enable RADVD
☒ Enable MLD Snooping
☐ Standard Mode
☒ Blocking Mode

Enable MLD LAN to LAN Multicast: Enable ▼
 (LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

☒ Enable Relay

DHCPv6 Server IP Address:

Selected WAN Interface: Default ▼

Hop limit:

Save/Apply

Figure 51 – IPv6 LAN Auto Configuration page

OPTION	DEFINITION
Enable Unique Local Addresses and Prefix Advertisement	Enable the use of unique local addresses. The gateway will advertise the IPv6 /64 prefix to new devices on the network.
Randomly Generate	Randomly generates the unique local addresses and the prefix.
Statically Configure	Enter a static IPv6 address for the gateway if one has been assigned to you by your Internet Service Provider (ISP).
IPv6 LAN Applications	Enable IPv6 DHCP server
Enable DHCPv6 Server or RADVD	The Gateway Advertisement Daemon (radvd) is an open-source software product that implements link-local advertisements of IPv6 gateway addresses and IPv6 routing prefixes using the Neighbour Discovery Protocol (NDP) as specified in RFC 2461. The Gateway Advertisement Daemon is used by system administrators in stateless auto-configuration methods of network hosts on Internet Protocol version 6 networks. When IPv6 hosts configure their network interfaces, they broadcast gateway solicitation (RS) requests onto the network to discover available gateways. The radvd software answers requests with gateway advertisement (RA) messages. In addition,

OPTION	DEFINITION
	radvd periodically broadcasts RA packets to the attached link to update network hosts. The gateway advertisement messages contain the routing prefix used on the link, the link maximum transmission unit (MTU), and the address of the responsible default gateway.
Stateless (for DHCPv6 Server)	IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) gateway discovery messages. This type of configuration is suitable for small organizations and individuals. It allows each host to determine its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address.
Stateful (for DHCPv6 Server)	This configuration requires some human intervention as it makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for installation and administration of nodes over a network. The DHCPv6 server maintains a list of nodes and the information about their state to know the availability of each IP address from the range specified by the network administrator.
Enable MLD Snooping	Select whether to enable or disable MLD Snooping on the gateway. The Multicast Listener Discovery (MLD) snooping function constrains the flooding of IPv6 multicast traffic on LANs on the gateway.
Enable Relay	When enabled, relays DHCP messages between DHCPv6 clients and DHCPv6 servers on different IPv6 networks.

Table 20 – IPv6 LAN Auto Configuration settings

LAN VLAN Setting

This page allows you to specify a LAN port to apply VLAN tagging to.

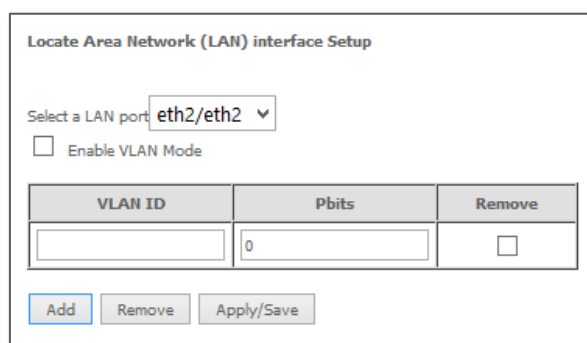


Figure 52 – Specify a LAN port for VLAN tagging

Select the LAN port using the drop down menu, then click the **Add** button.

Enter the **VLAN ID** and in the **Pbits** field enter a value from 0-7 indicating the priority of the VLAN.

Click **Apply/Save** when you have finished.

Virtual Servers

Virtual Servers (also commonly referred to as port forwarding) allow you to direct incoming traffic from the WAN side to the Internal network host with a private IP address on the LAN side.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	LAN Loopback	Enable/Disable	Remove
Flight Simulator 2000	2300	2400	UDP	2300	2400	192.168.20.6	eth4.1	Enabled	<input type="checkbox"/>	<input type="checkbox"/>
CART Precision Racing	47624	47624	TCP	47624	47624	192.168.20.2	lte0	Disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 53 – NAT -- Virtual Server list

Click the **Add** button to add a virtual server.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
 Remaining number of entries that can be configured:30

Use Interface:

Service Name:

☒ Select a Service:

☐ Custom Service:

☒ Enable LAN Loopback

Server IP Address:

Status:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
47624	47624	TCP ▼	47624	47624
6073	6073	TCP ▼	6073	6073
2300	2400	TCP ▼	2300	2400
2300	2400	UDP ▼	2300	2400
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		

Figure 54 – NAT -- Virtual Server Configuration page

FIELD	DESCRIPTION
Select a Service or Custom Service	Select a pre-configured port forwarding rule or choose custom server to create your own port forwarding rule.
Enable LAN Loopback	Select <input checked="" type="checkbox"/> Enable LAN Loopback to make the virtual server available on the LAN side. In this way the user on the LAN side can access service

FIELD	DESCRIPTION
	on the LAN side using the WAN IP address and configured external port.
Server IP Address	Enter the IP address of the local server/host.
External Port Start	Enter the starting external port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.
External Port End	Enter the ending external port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.
Protocol	Options include: TCP, UDP or TCP/UDP
Internal Port Start	Enter the starting internal port number range(when custom server is selected). When a predefined service is selected this field will be completed automatically.
Internal Port End	Enter the ending internal port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.

Table 21 – NAT – Virtual Server settings table

Click **Save/Apply** to save your settings when you have finished creating virtual servers.

Port Triggering

Some applications require specific ports in the gateway's firewall to be open for access by remote parties. Port Triggering opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'.

The Gateway allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

This is a list of specific ports in the gateway's firewall that are open for access by remote parties.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum **32** entries can be configured.

Due to limited resources, port triggering feature has some limitation:
sum of the outports of all configuration entries <= 1000
sum of the inports of one configuration entry <= 1000

Application Name	Trigger		Open			WAN Interface	Remove	
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		
Rainbow Six/Rogue Spea	TCP	2346	2346	TCP/UDP	2436	2438	eth4.1	<input type="checkbox"/>

Add
Remove

Figure 55 – NAT -- Port Triggering list

Click the **Add** button and configure the port settings from an existing application in the drop-down list or create your own custom application.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.
Remaining number of entries that can be configured:

Use Interface: ETH WAN/eth4.1 ▼

Application Name:

☐ Select an application: Calista IP Phone ▼

☒ Custom application: CalPort005

Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
5190	5190	TCP/UDP ▼	3000	3000	TCP/UDP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼

Apply/Save

Figure 56 – NAT -- Port Trigger Configuration page

FIELD	DESCRIPTION
Select an Application or Custom Application	A user can select a pre-configured application from the list or select the Custom Application option to create custom application settings.
Trigger Port Start	Enter the starting trigger port number (when you select <input checked="" type="radio"/> Custom Application). When an application is selected the port range values are automatically entered.
Trigger Port End	Enter the ending trigger port number (when you select <input checked="" type="radio"/> Custom Application). When an application is selected the port range values are automatically entered.
Trigger Protocol	Options include: TCP, UDP or TCP/UDP
Open Port Start	Enter the starting open port number (when you select <input checked="" type="radio"/> Custom Application). When an application is selected the port range values are automatically entered.
Open Port End	Enter the ending open port number (when you select <input checked="" type="radio"/> Custom Application). When an application is selected the port range values are automatically entered.
Open Protocol	Options include: TCP, UDP or TCP/UDP

Table 22 – NAT -- Port Trigger Configuration settings

DMZ Host

The NL1901ACV will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table or being used in the Virtual Server table to the DMZ host.

Enter the **Host's IP address** and click **Apply** to activate the DMZ host. To deactivate the DMZ Host function, clear the IP address field and press the **Save/Apply** button.

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

☒ Enable LAN Loopback

Apply/Save

Figure 57 – NAT – DMZ Host settings

Note that ☒ **Enable LAN Loopback** can also be selected.

LAN Loopback allows the LAN host to access another LAN host/server via the external IP Address of the gateway. Without NAT loopback you must use the internal IP address of the device when on the LAN side.

ALG

The Application Layer Gateway (ALG) is a feature which enables the gateway to parse application layer packets and support address and port translation for certain protocols. We recommend that you leave these protocols enabled unless you have a specific reason for disabling them.

ALG

Select the ALG below.

☒ FTP Enabled

☒ SIP Enabled

☒ TFTP Enabled

☒ H323 Enabled

☒ IRC Enabled

☒ Port Triggering Enabled

☒ PPTP Enabled

☒ IPSEC Enabled

☒ RTSP Enabled

Save/Apply

Figure 58 – NAT – Application Layer Gateway (ALG) settings

Security

IP Filtering

The gateway supports IP Filtering which allows you to easily set up rules to control incoming and outgoing Internet traffic. The gateway provides two types of IP filtering: **Outgoing IP Filtering** and **Incoming IP Filtering**

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	Source IP/ Prefix Length	Source Port	Destination IP/ Prefix Length	Destination Port	Remove
<div> Add Remove </div>							

Figure 59 – IP Filtering List – Block outgoing traffic

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	Source IP/ Prefix Length	Source Port	Destination IP/ Prefix Length	Destination Port	Remove
<div> Add Remove </div>								

Figure 60 – IP Filtering List – Accept incoming traffic

Outgoing IP Filtering

By default, the gateway allows all outgoing Internet traffic from the LAN but by setting up Outgoing IP Filtering rules, you can block some users and/or applications from accessing the Internet.

To delete the rule, click ☒ in the **Remove** column next to the selected rule and then click the **Remove** button.

To create a new outgoing IP filter, click **Add**. The Add IP Filter-Outgoing page will be displayed.

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Figure 61 –Outgoing IP Filter settings

PARAMETER	DEFINITION
Filter Name	Enter a name to identify the filtering rule.
IP Version	Select the IP version to apply the filter to. (IPv4/IPv6)
Protocol	Select the protocol type to block (UDP/TCP/Both)
Source IP Address/Subnet Mask	Enter the IP Address of the host on the LAN to block
Source Port	Enter the port number used by the application to block
Destination IP Address/Subnet Mask	Enter the IP Address of the Remote Server/host to which connections should be blocked
Destination Port	Enter the destination port number used by the application to block

Table 23 – Outgoing IP Filter settings table

Click **Apply/Save** to take effect the settings. The new rule will then be displayed in the Outgoing IP Filtering table list.

Incoming IP Filtering

By default, when NAT is enabled, all incoming IP traffic from WAN is blocked except for responses to requests from the LAN. However, some specific incoming traffic from the Internet can be accepted by setting up Incoming IP Filtering rules.

To delete the rule, click ☒ in the **Remove** column next to the selected rule and click the **Remove** button.

To create a new incoming IP filter, click **Add**. The Add IP Filter-Incoming page will be displayed.

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☒ Select All
☒ Great/ipoa0
☒ ETH WAN/eth4.1
☒ VDSL/ppp0.1
☒ br0/br0

Figure 62 – Incoming IP Filter settings

Enter the following parameters:

PARAMETER	DEFINITION
Filter Name	Enter a name to identify the filtering rule
IP Version	Select the IP version to apply the filter to

PARAMETER	DEFINITION
Protocol	Select the protocol type to allow
Source IP Address/ Subnet Mask	Enter the IP Address of the Remote Server/Host from which to allow connections
Source Port	Enter the port number used by the application to allow
Destination IP Address/ Subnet Mask	Enter the IP Address of the Host on the LAN to which connections should be allowed
Destination Port	Enter the destination port number used by the application to allow
WAN Interface	Select the WAN Interface to apply the filter to

Table 24 – Incoming IP Filter settings table

Click **Save/Apply** to take effect the settings. The new rule will then be displayed in the Incoming IP Filtering table list.

MAC Filtering

The NL1901ACV offers the ability to use MAC Address filtering on ATM PVCs. You can elect to block or allow connections based on MAC Address criteria. The default policy is to allow all connections.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface (maximum 32 entries):
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
ptm0.2	BLOCKED	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ptm0.2	PPPoE	1a:11:21:c2:c3:aa	1a:23:24:c2:c3:11	BOTH	<input type="checkbox"/>

Figure 63 – Security – MAC Filter list

Click **Add** to enter a new MAC Address filter.

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click 'Apply' to save and activate the filter.

Protocol Type: PPPoE ▼

Destination MAC Address: 1a:11:21:c2:c3:aa

Source MAC Address: 1a:23:24:c2:c3:11

Frame Direction: LAN<=>WAN ▼

WAN Interfaces (Configured in Bridge mode only)

VDSL/ptm0.2 ▼

Apply/Save

Figure 64 – Security – MAC Filter settings

- 1 Enter the **Protocol type** to which the filter should apply.
- 2 Enter the **Source** and **Destination MAC Address**
- 3 Enter the **Frame Direction** of the traffic to filter
- 4 Select the **WAN interface** to which the filter should apply.

Click **Apply/Save** to save the new MAC filtering configuration.

Parental Control

The Parental Control feature allows you to take advanced measures to ensure the computers connected to the LAN are used only when and how you decide.

Time Restriction

This Parental Control function allows you to restrict access from a Local Area Network (LAN) connected device to an outside network through the gateway on selected days and at certain times. Make sure to activate the Internet Time server synchronization as described in the SNTP section, so that the scheduled times match your local time.

Access Time Restriction -- A maximum 16 entries can be configured.

Rule Name	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
AfterSchool	ec:08:6b:02:aa:0a	x	x	x	x	x			13:00	20:00	<input type="checkbox"/>
DaytimeSatSun	ec:08:6b:02:aa:0a						x	x	09:00	16:30	<input type="checkbox"/>

Add
Remove

Figure 65 – Advanced – Parental Control – Time Restriction

To add a time restriction rule, press the **Add** button.

The following screen appears.

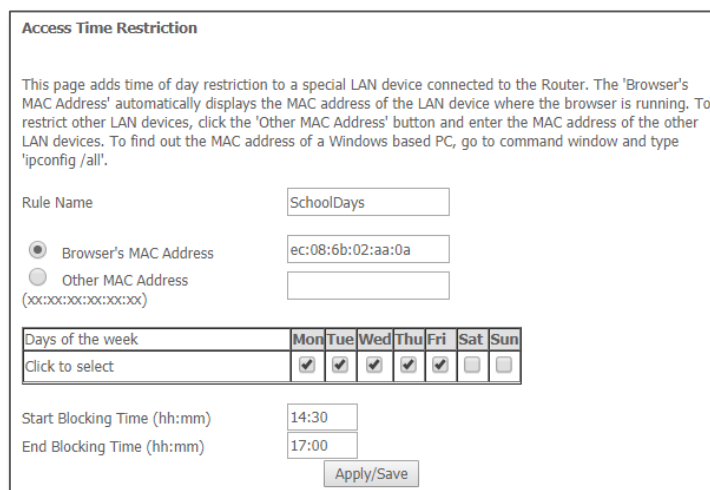


Figure 66 – Advanced – Parental Control – Add Time Restriction

FIELD	DESCRIPTION
Rule Name	A user defined name for the time restriction rule.
Browser's MAC Address	The MAC address of the network card of the computer running the browser.
Other MAC Address	The MAC address of another LAN device or network card.
Days of the Week	The days of the week for which the rules apply.
Start Blocking Time	The time of day when the restriction starts. (24 hour time: 00:00–23:59)
End blocking time	The time of day when the restriction ends. (24 hour time: 00:00–23:59)
Apply/Save button	Press the Apply/Save button to save a time restriction rule.

Table 25 – Advanced – Parental Control – Add Time Restriction Settings

URL Filter

With the URL filter, you are able to add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the NL1901ACV.

Select the **Black List** (to block) or **White List** (to allow) option and then click **Add** to enter the URL you wish to add to the URL Filter list.

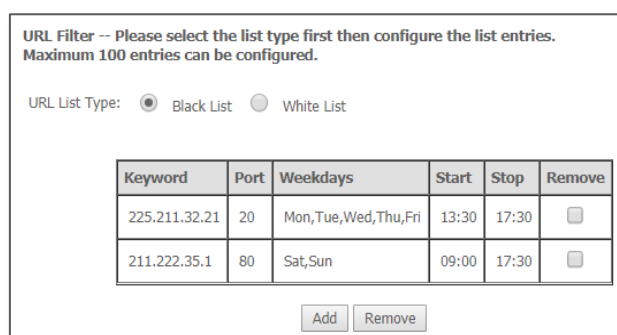


Figure 67 – Advanced – Parental Control – URL Filter


FIELD	DESCRIPTION
URL List Type	Select <input checked="" type="radio"/> Black List to <u>prevent any</u> website containing the Keyword string in its URL from accessing your entire local area network during the set time period. Select <input type="radio"/> White List to <u>allow only</u> websites containing one of the Keyword strings in its URL to accessing your local area network .
Keyword	Keywords can be: <ul style="list-style-type: none"> • a URL address – e.g. www.facebook.com • an IP address – e.g. 226.58.199.68 or <ul style="list-style-type: none"> • string of characters – e.g. 'adult', 'XXX' <div>  Attention – The string of characters Keyword approach will not work for websites that are secured using the https (Hyper Text Transfer Protocol Secure) protocol. Therefore any website with https:// in its URL will not be blocked using keyword(s) filters containing strings of text or characters. </div>
Port Number	Enter the port number, the default port 80 will be applied if this is left blank.
Days of the Week	Select the <input checked="" type="checkbox"/> days of the week for which the black or white list will be applied to the filtered URLs.
Start Time	The Start time expressed in 24 hour time settings.
End time	The Stop time expressed in 24 hour time settings.
Remove	To permanently delete a filter from the list, select its <input checked="" type="checkbox"/> checkbox in the Remove column and click the Remove button.
Add button	Press the Add button to open the filter creation dialog.

Table 26 – Advanced – Parental Control – Add URL Restriction Settings

Once you have chosen to add a URL to the list you will be prompted to enter the address. Simply type it in and select the **Apply/Save** button.

Parental Control -- URL Filter Add
Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.

URL Address:
Port Number: (Default 80 will be applied if leave blank.)

Days of the week
Click to select

Mon	Tue	Wed	Thu	Fri	Sat	Sun
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Start Time (hh:mm)
End Time (hh:mm)

Figure 68 – Advanced – Parental Control – Add URL Filter

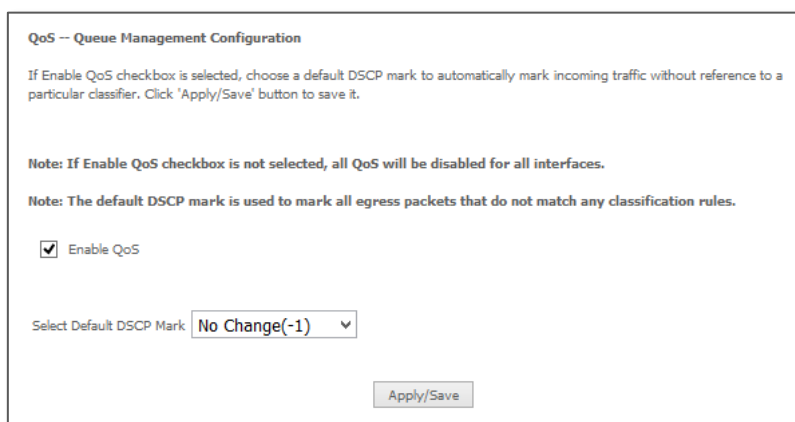
FIELD	DESCRIPTION
URL Address	The URL address of the device you want to black list or white list. This can also be an IP Address or a keyword(s) which are character strings. Note that character string keyword filters will not work on websites that are secured using the https (Hyper Text Transfer Protocol Secure) protocol.
Port Number	The Port Number (Default is 80).

FIELD	DESCRIPTION
Days of the Week	Select the <input checked="" type="checkbox"/> days of the week for which the rule will apply.
Start Time	The time of day when the restriction starts. (24 hour time: 00:00–23:59)
End time	The time of day when the restriction ends. (24 hour time: 00:00–23:59)
Apply/Save button	Press the Apply/Save button to save a URL based time restriction rule.

Table 27 – Advanced – Parental Control – Add URL Restriction Settings

Quality of Service

Quality of Service offers a defined level of performance in a data communications system - for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video streaming is not disrupted by other network traffic. This means that if you are streaming video and someone else in the house starts downloading a large file, the download won't disrupt the flow of video traffic.



QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☒ Enable QoS

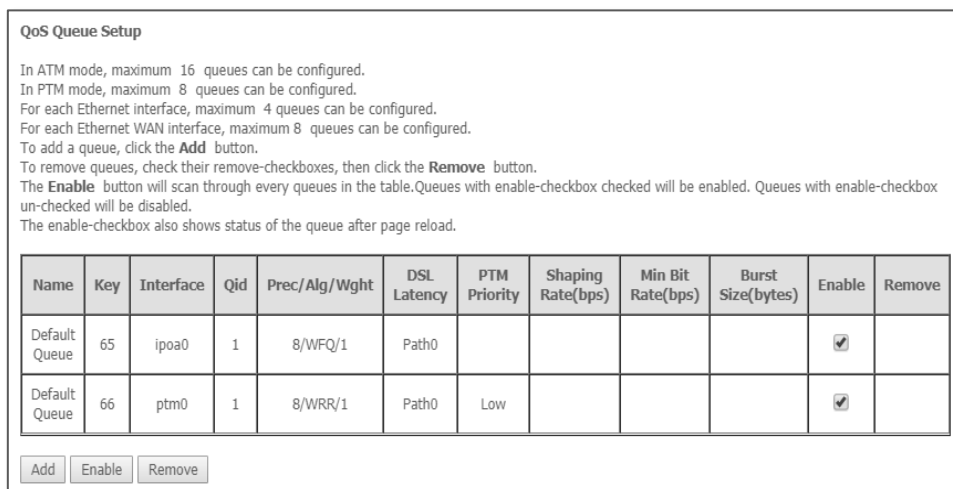
Select Default DSCP Mark: No Change(-1) ▼

Apply/Save

Figure 69 – Advanced – Enable QoS

To enable QoS select the **Enable QoS** checkbox, and set the **Default DSCP (Differentiated Services Code Point) Mark**. Then press the **Apply/Save** button.

QoS Queue



QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
 In PTM mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 4 queues can be configured.
 For each Ethernet WAN interface, maximum 8 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate(bps)	Min Bit Rate(bps)	Burst Size(bytes)	Enable	Remove
Default Queue	65	ipoa0	1	8/WFQ/1	Path0					<input checked="" type="checkbox"/>	
Default Queue	66	ptm0	1	8/WRR/1	Path0	Low				<input checked="" type="checkbox"/>	

Add Enable Remove

Figure 70 – Advanced – QoS Queue Setup

Click the **Add** button to add a QoS Queue. The following screen is displayed.

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Name:

Enable: Enable ▼

Interface: eth4(wan) ▼

Queue Precedence: 1(SP) ▼ (lower value, higher priority)

- The precedence list shows the scheduler algorithm configured at each precedence level.
 - Note that precedence level with SP scheduler may have only one queue.
 - precedence level with WRR/WFQ scheduler may have multiple queues.

Minimum Rate: [1-1000000 Kbps] (-1 indicates no shaping)

Shaping Rate: [1-1000000 Kbps] (-1 indicates no shaping)

Shaping Burst Size: [bytes] (shall be >=1600)

Figure 71 – Advanced – QoS – Add QoS Queue

The above screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately.



Note – Precedence level 1 relates to higher priority while precedence level 3 relates to lower priority, etc.

WLAN Queue

The **QoS WLAN Queue** page displays a summary of the QoS configuration.

QoS Wlan Queue Setup

Note: If WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	Enable
WMM Voice Priority	1	wl0	8	1/SP	Enabled
WMM Voice Priority	2	wl0	7	2/SP	Enabled
WMM Video Priority	3	wl0	6	3/SP	Enabled
WMM Video Priority	4	wl0	5	4/SP	Enabled
WMM Best Effort	5	wl0	4	5/SP	Enabled
WMM Background	6	wl0	3	6/SP	Enabled
WMM Background	7	wl0	2	7/SP	Enabled
WMM Best Effort	8	wl0	1	8/SP	Enabled

Figure 72 – Advanced – QoS – WLAN Queue

QoS Classification

QoS Classification Setup -- A maximum 32 entries can be configured.

To add a rule, click the **Add** button.
 To remove rules, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS									
Class Name	Order	Class Interface	Ethernet Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Prefix Length	Destination	Min/Max/IpLength	Protocol	Source Port	Destination	DSCP Check	802.1P Check	TC Check	Queue Key	DSCP Mark	802.1P Mark	TC Mark	Rate Limit(kbps)	Enable	Remove		
																					<input type="button" value="Add"/>	<input type="button" value="Enable"/>	<input type="button" value="Remove"/>

Figure 73 – Advanced – QoS Classification list

Click the **Add** button to configure network traffic classes.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria A blank criterion indicates it is not used for classification.

Ingress Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Egress Interface (Required):

Specify Egress Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit(kbps): [Kbits/s]

Figure 74 – Advanced – QoS – Network Traffic Class settings

The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click the **Apply/Save** button to save and activate the rule.

QoS Port Shaping

Port Shaping allows the limiting of continuous network speed without affecting burst traffic. For example, when your browser loads a web page, this is a type burst traffic as the browser aims to fetch small amounts of data quickly and then leaves the connection idle. Limiting port speed alone will affect the speed at which web pages are loaded, causing users to feel that their overall internet connection speed is slow.

By configuring QoS Port Shaping with a Burst size, web pages are allowed to load using the burst speed, while continuous traffic such as file downloads will be shaped at a lower rate.

To identify the best way to configure shaping rate and burst size, consider the equation below:

$$\text{Time window} = \text{Burst size} / \text{rate}$$

For example, if a 200 Mbps bandwidth limit is configured with a 5 ms burst window, the calculation becomes 200 Mbps x 5 ms = 125 Kbytes, which is approximately eighty-three (83) 1500-byte packets. If the 200 Mbps bandwidth limit is configured on a Gigabit Ethernet interface, the burst duration is 125000 bytes / 1 Gbps = 1 ms at the Gigabit Ethernet line rate.

After 1ms of burst data at full gigabit speed, the speed is shaped to 200Mbps.

QoS Port Shaping Setup

QoS port shaping supports traffic shaping of Ethernet interface.
If Shaping Rate is set to -1, it means no shaping and Burst Size will be ignored.

Interface	Type	Shaping Rate (Kbps)	Burst Size (bytes)
eth4	WAN	<input type="text" value="-1"/>	<input type="text" value="0"/>
eth0	LAN	<input type="text" value="-1"/>	<input type="text" value="0"/>
eth1	LAN	<input type="text" value="-1"/>	<input type="text" value="0"/>
eth2	LAN	<input type="text" value="-1"/>	<input type="text" value="0"/>
eth3	LAN	<input type="text" value="-1"/>	<input type="text" value="0"/>

Figure 75 – QoS Port Shaping settings

ITEM	DESCRIPTION
Interface	Identifies the interface type.
Type	Identifies the connection type.
Shaping Rate	The speed you would limit the port to in Kbps (Kilobits per second) after the burst size.
Burst Size	Burst size should be more than 10x MTU (>=15000 bytes)
Apply/Save button	Click to save and apply your changes

Figure 76 – Advanced – QoS – Port Shaping settings



Note: 1 byte = 8 bits

Routing

The Default Gateway, Static Route, Policy Routing and Dynamic Route settings can be found in the Routing option of the Advanced menu.

Default Gateway

Select your preferred WAN interface from the available options.

Use the arrow buttons to move the available Routed WAN Interfaces listed on the right to the group of required **Default Gateway Interfaces** in the list on the left.

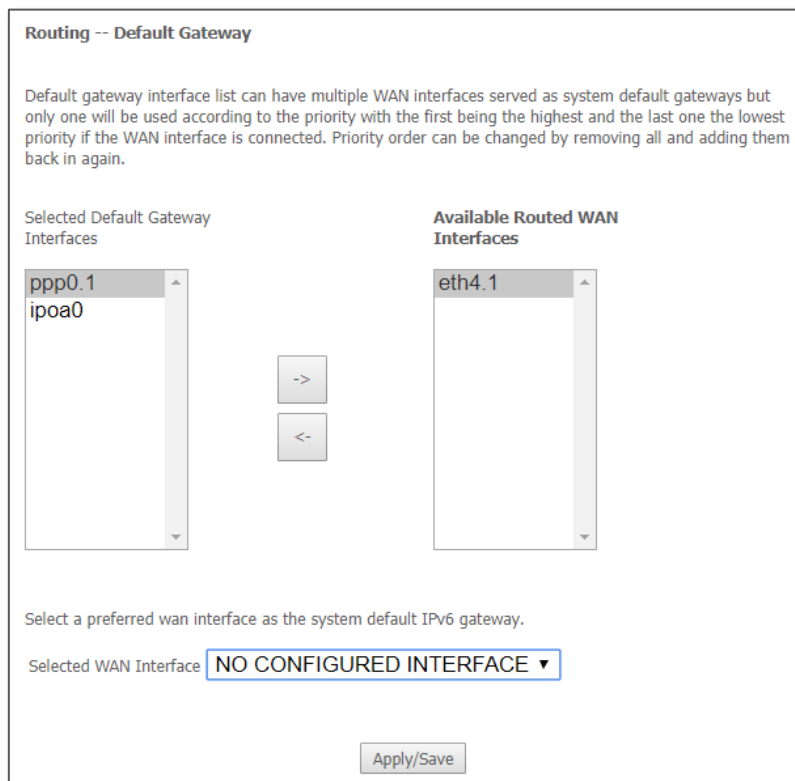


Figure 77 – Routing – Set Default Gateway

Use the arrow buttons to move the interfaces required as DNS Server interfaces to the left.

The interface highest on the list has the highest priority as a DNS server.

Click **Apply/Save** to commit your settings to the gateway.

Static Route

The Static Route screen displays the configured static routes. Click the **Add** or **Remove** buttons to change settings.

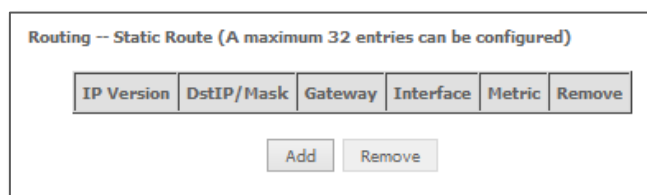
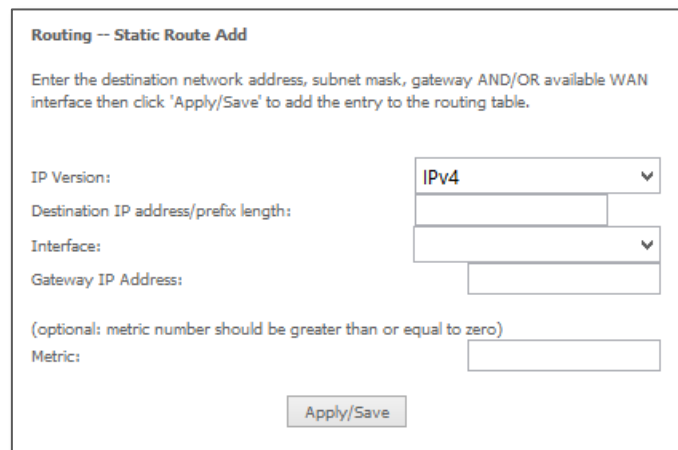


Figure 78 – Routing – Static Route list

To add a static route rule click the **Add** button. The following screen is displayed.



Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Apply/Save' to add the entry to the routing table.

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

Figure 79 – Routing – Static Route configuration

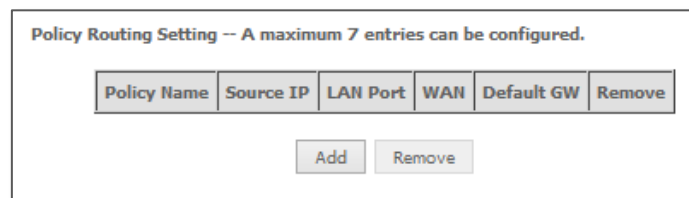
Select the **IP Version**, enter the **Destination Network Address**, select an **Interface**, and enter the **Gateway IP Address**.

Optionally enter a number in the **Metric** field to set a priority for this route, the lower the number the higher the priority.

Then click **Apply/Save** to add the entry to the routing table.

Policy Routing

This function allows you to add policy rules to certain situations.

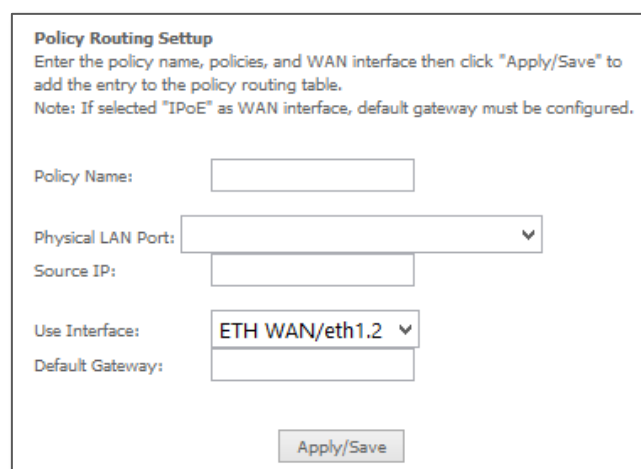


Policy Routing Setting -- A maximum 7 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Figure 80 – Routing – Policy Routing list

Click the **Add** button to add a policy rule. The following screen is displayed.



Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.

Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface: ETH WAN/eth1.2

Default Gateway:

Figure 81 – Advanced – Routing – Policy Route configuration

Enter the details into the provided fields. The table below describes each field.

FIELD	DESCRIPTION
Policy Name	A user defined name for the policy route.
Physical LAN Port	The LAN port to be used for the policy.
Source IP	The IP address of the LAN device involved with the policy.
Use Interface	Select the Interface that the policy will employ.
Default Gateway	Enter the gateway address.

Table 28 – Routing – Policy Route settings table

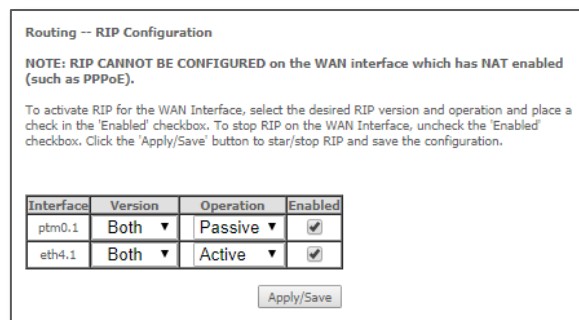
RIP

The Routing Information Protocol (RIP) allows gateways to exchange network topology information. This information allows the automatic creation and updating of routing tables.



Attention – RIP cannot be selected for a WAN interface which is NAT enabled, such as PPPoE.

Go to **Basic Setup** and select **Ethernet WAN**, click **Next** and then select **IP over Ethernet (IPoE)**. The RIP option will now be available.



Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to start/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
ptm0.1	Both ▼	Passive ▼	<input checked="" type="checkbox"/>
eth4.1	Both ▼	Active ▼	<input checked="" type="checkbox"/>

Apply/Save

Figure 82 – Routing – RIP list

ITEM	DESCRIPTION
Interface	The network interface that the RIP settings apply to.
Version	1 – Use RIPv1 to support classful routing. 2 – Use RIPv2 to support subnet information gathering and Classless Inter-Domain Routing. Both – RIP will use both RIPv1 & RIPv2 , and will multicast and broadcast to all adjacent gateways.
Operation	Passive – RIP will only respond to “Request Message” queries on the RIP enabled interface. Active – RIP will broadcast and respond to “Request Message” queries on the RIP enabled interface.
Enabled	Select <input checked="" type="checkbox"/> Enabled to activate the RIP routing service on the selected Interface.
Apply/Save button	Click the Apply/Save button to initiate the change.

Table 29 – Routing – RIP settings

DNS Server Configuration

A DNS server is a server that contains a database of hostnames and their associated public IP addresses.

This server is used to resolve hostnames to a unique public IP address when requested.

When a user enters a URL e.g. www.netcommwireless.com into their browser, your gateway is contacting the DNS server and requesting the webserver IP address.

Hostname URLs are easier for humans to understand and remember than IP address numbers. A host's IP addresses can change from time to time hence a DNS server is required to locate and translate a hostname.

DNS Servers can be used to block unwanted content, such as explicit material. By using a filtered DNS server, the hostname of these materials will not be resolved, allowing parental control to accessible content.

Parental Control DNS are available as a free service or customizable paid service. For example: OpenDNS FamilyShield, Norton ConnectSafe, Yandex.DNS, Comodo Secured, etc.

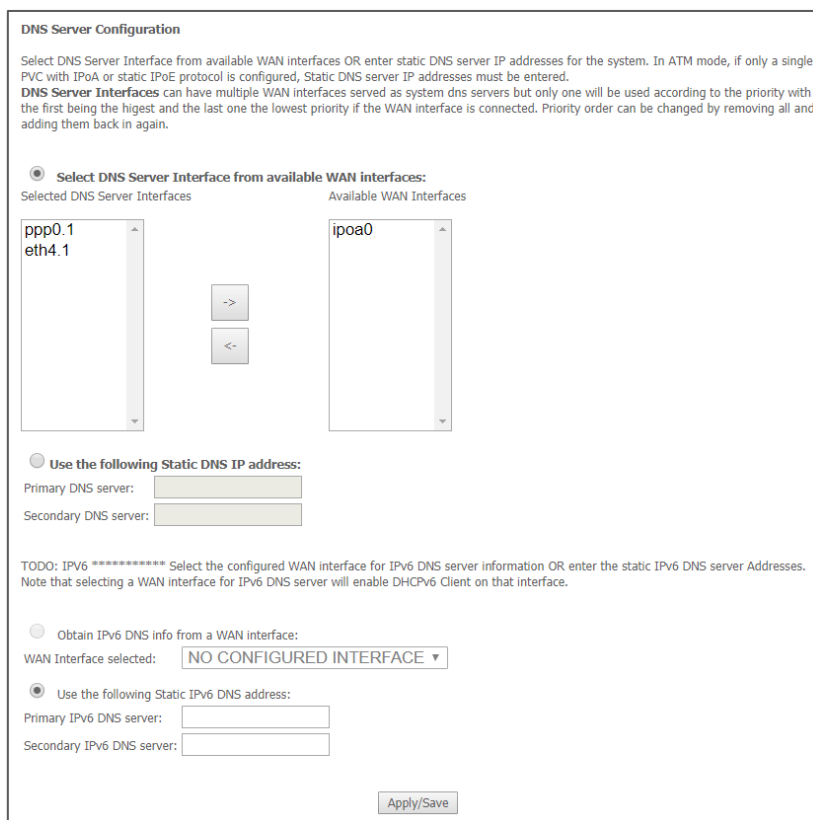


Figure 83 – DNS Server Configuration

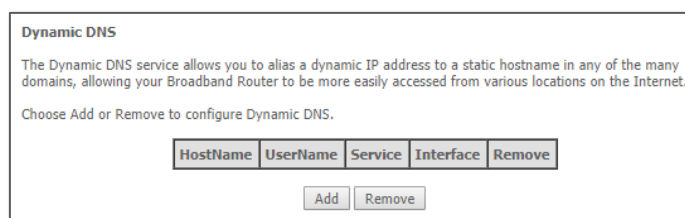
FIELD	DESCRIPTION
DNS server via interface	Use DNS server provided from your ISP automatically from the assigned interface. Use the arrow to select the WAN interface to request DNS server, with the first being the highest priority.
Static DNS IP Address	Specify your own Primary and Secondary DNS server.

FIELD	DESCRIPTION
IPv6 DNS info from WAN interface	Use IPv6 DNS server provided from your ISP automatically from the assigned interface.
Static IPv6 DNS IP Address	Specify your own Primary and Secondary IPv6 DNS server.
Apply/Save Button	Click the Apply/Save button to initiate the change.

Table 30 – Routing – RIP settings

Dynamic DNS

When you have an Internet plan that provides a dynamic IP address, that is, an address which is dynamically assigned and changes each time you connect, an easy way to provide a permanent address is to use a Dynamic DNS service. There are both free and paid DDNS services available.



Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

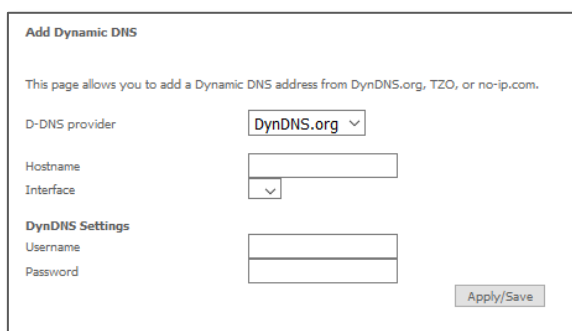
Choose Add or Remove to configure Dynamic DNS.

HostName	UserName	Service	Interface	Remove
<div> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>				

Figure 84 – Dynamic DNS list

To add a new Dynamic DNS profile, click the **Add** button. The Add Dynamic DNS screen is displayed.

- 1 From the D-DNS provider drop down list, select your Dynamic DNS provider.
- 2 In the **Hostname** field, enter the dynamic DNS hostname.
- 3 Use the **Interface** drop down list to select the interface that the service should operate on.
- 4 Enter the username and password for your dynamic DNS account.
- 5 Click **Apply/Save**.



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org, TZO, or no-ip.com.

D-DNS provider: DynDNS.org

Hostname:

Interface: ▼

DynDNS Settings

Username:

Password:

Figure 85 – Add Dynamic DNS

DSL

This page allows you to modify the DSL modulation settings on the unit. By changing the settings, you can specify which DSL modulation that the gateway will use.

Not all modulation types are support by your local DSLAM equipment, check with your ISP for supported modulation types.

DSL Settings

Select the modulation below.

- ☒ G.Dmt Enabled
- ☒ G.lite Enabled
- ☒ T1.413 Enabled
- ☒ ADSL2 Enabled
- ☒ AnnexL Enabled
- ☒ ADSL2+ Enabled
- ☐ AnnexM Enabled
- ☒ VDSL2 Enabled

Select the profile below.

- ☒ 8a Enabled
- ☒ 8b Enabled
- ☒ 8c Enabled
- ☒ 8d Enabled
- ☒ 12a Enabled
- ☒ 12b Enabled
- ☒ 17a Enabled

US0

☒ Enabled

Select the phone line pair below.

☒ Inner pair
☐ Outer pair

Capability

☒ Bitswap Enable
☒ SRA Enable

Figure 86 – DSL settings page

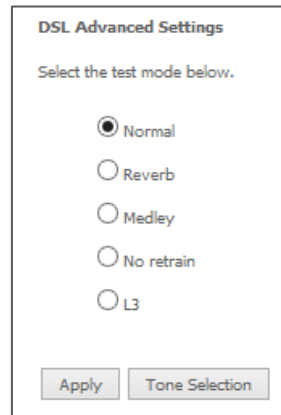
FIELD	DESCRIPTION
Modulation	A user defined name for the policy route.
Profile	The LAN port to be used for the policy.
US0	The IP address of the LAN device involved with the policy.
Phone line type	Select the Interface that the policy will employ.
Capability	Enter the gateway address.
Apply/Save button	Click the Apply/Save button to initiate the change.
Advanced Settings button	Allow configuration of the Gateway state for diagnostic purposes.

Table 31 – DSL settings table

DSL Advanced settings

For advanced DSL options press the **Advanced Settings** button.

The DSL advanced settings relate to test mode settings. The default selection is **Normal**.



The image shows a dialog box titled "DSL Advanced Settings". Inside, it says "Select the test mode below." and lists five radio button options: "Normal" (which is selected), "Reverb", "Medley", "No retrain", and "L3". At the bottom of the dialog are two buttons: "Apply" and "Tone Selection".

Figure 87 – DSL Advanced Settings page

FIELD	DESCRIPTION
Normal	Puts the gateway in normal operation mode. The default setting.
Reverb	Puts the gateway in a test mode in which it only sends a Reverb signal.
Medley	Puts the gateway in a test mode in which it only sends a Medley signal.
No retrain	In this mode, the gateway will try to establish a connection as in normal mode, but once the connection is up it will not retrain if the signal is lost.
L3	Puts the gateway in the Link state (Idle) at the start of the initialization procedure.
Apply button	Click the Apply button to initiate the change.
Tone Selection button	Allow selection of frequency band for data transfer.

Table 32 – DSL settings table

ADSL Tone Settings

To alter the ADSL Tone Settings, click the **Tone Selection** button on the *DSL Advanced Settings* page.

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125kHz apart. With each tone carrying separate data, the technique operates as if 256 separate gateways were running in parallel. The tone range is from 0 to 31 for upstream traffic and from 32 to 255 for downstream traffic.

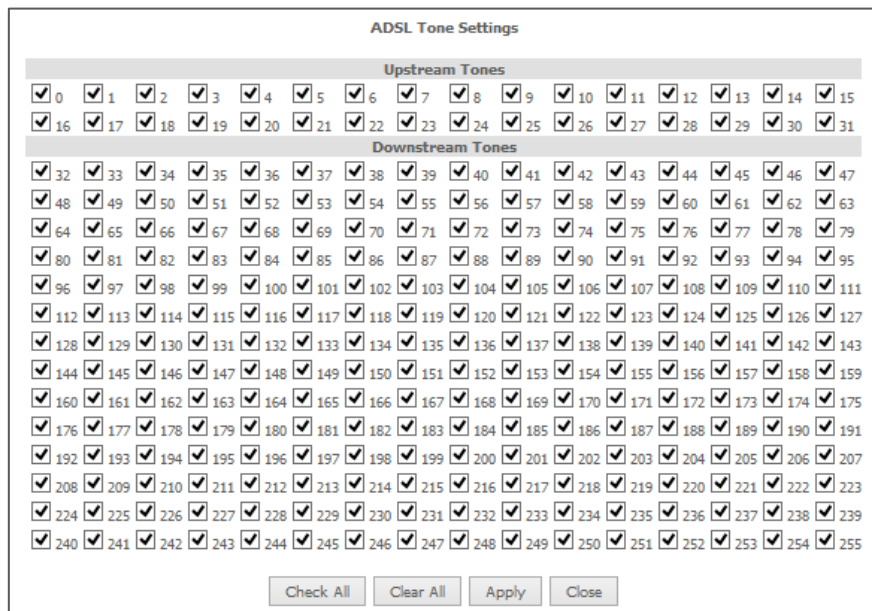


Figure 88 – ADSL Tone Settings page



Warning – Do not change these settings unless you are directed to by your Internet Service Provider.

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, gaming console, WiFi access points and mobile phones to automatically detect each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

Select ☒ **Enable UPnP** and then click the **Apply/Save** button to allow automatic port forwarding configuration detection for your UPnP devices.

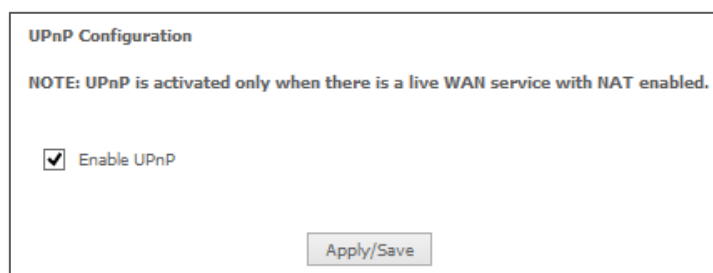


Figure 89 – UPnP activation page



Note – This **UPnP** functionality is only available when there is a live **WAN** service with **NAT** enabled.

DNS Proxy

To enable DNS Proxy settings, select ☒ **Enable DNS Proxy** and then enter the **Host name of the Broadband Gateway** and **Domain name of the LAN network**, as in the example shown below. Click **Apply/Save** to continue.

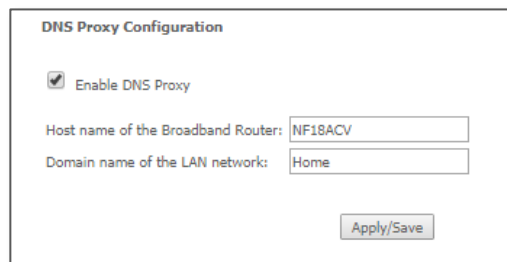


Figure 90 – DNS Proxy activation page

The Host name and Domain name are combined to form a unique label that is mapped to the gateway IP address. This can be used to access the user interface of the gateway with a local name rather than by using the gateway IP address. For example, you can access your gateway by entering `http://NL1901ACV` into your web browser.

DLNA

The DLNA page allows you to enable or disable and configure the digital media server. This means you can have digital media stored on an external USB hard drive connected to the NL1901ACV and the gateway will make it accessible to other devices on your network.

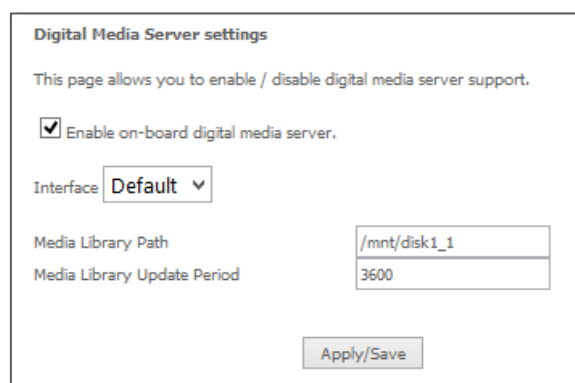


Figure 91 – DLNA setting page

Select ☒ **Enable on-board digital media server** and then use the drop down list to select the **Interface**. In the **Media Library Path** field, enter the path to the media and then enter a period between media library updates in seconds.

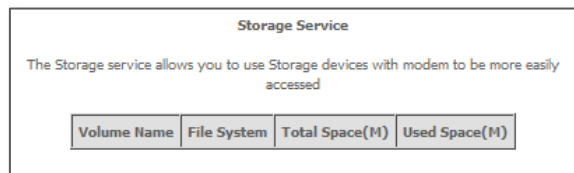
Click the **Apply/Save** button when you have finished.

Storage Service

The Storage Service options enable you to manage attached USB Storage devices and create accounts to access the data stored on the attached USB device.

Storage Device Info

The storage device info page displays information about the attached USB Storage device.



Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volume Name	File System	Total Space(M)	Used Space(M)
-------------	-------------	----------------	---------------

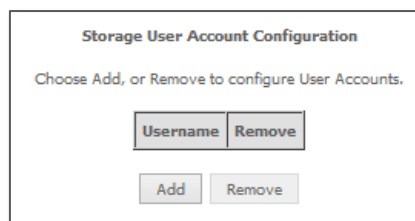
Figure 92 – Storage Device Info list

User Accounts

User accounts are used to restrict access to the attached USB Storage device.

To delete a User account entry, click the **Remove** checkbox next to the selected account entry and click **Remove**.

Click **Add** to create a user account.



Storage User Account Configuration

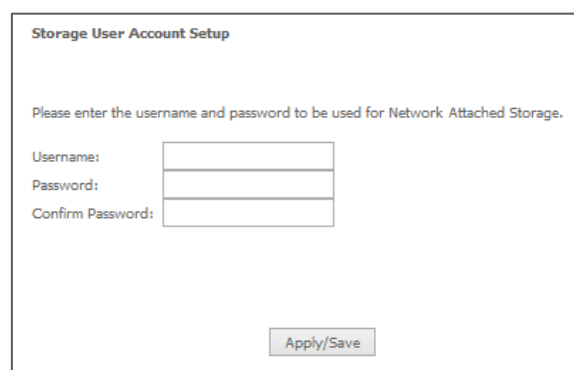
Choose Add, or Remove to configure User Accounts.

Username	Remove
----------	--------

Add Remove

Figure 93 – Storage User Accounts list

Adding an account allows the creation of specific user accounts with a password to further control access permissions. To add an account, click the **Add** button and then enter the desired username and password for the account.



Storage User Account Setup

Please enter the username and password to be used for Network Attached Storage.

Username:

Password:

Confirm Password:

Apply/Save

Figure 94 – Storage User Account Setup page

Interface Grouping

Port Mapping allows you to create groups composed of the various interfaces available in your gateway. These groups then act as separate networks.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces
Default	<input type="checkbox"/>	eth4.1 ptm0.2	eth0.0 eth1.222 eth1.786 eth3.100 eth3.200 eth3.789 wl0/5G wl1/2.4G
WorkGroup075	<input checked="" type="checkbox"/>	ppp0.1	eth1.0 eth2.0 eth3.0

Add Remove

Figure 95 – Interface Grouping list

Click **Add** to create an Interface group, see next section.

To delete an Interface group entry, click the ☒ checkbox next to the selected group entry and click the **Remove** button.

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
3. Click Save/Apply button to make the changes effective immediately.

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces

Available LAN Interfaces

eth0.0
eth1.0
eth2.0
eth3.0
wlan0
wlan1

Apply/Save

Figure 96 – Interface Grouping configuration

Enter a group name and then use the arrow buttons to select which interfaces you wish to group.

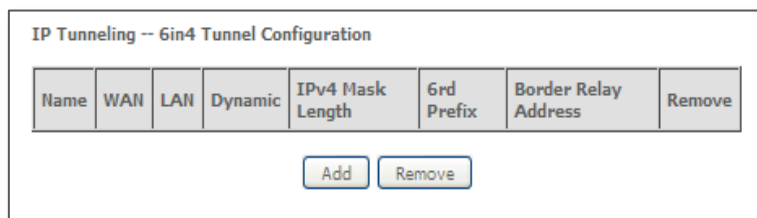
Click **Apply/Save** to save the Interface grouping configuration settings.

IP Tunnel

The IP Tunnelling feature allows you to configure tunnelling of traffic between IPv6 and IPv4 network using a tunnelling service.

IPv6inIPv4

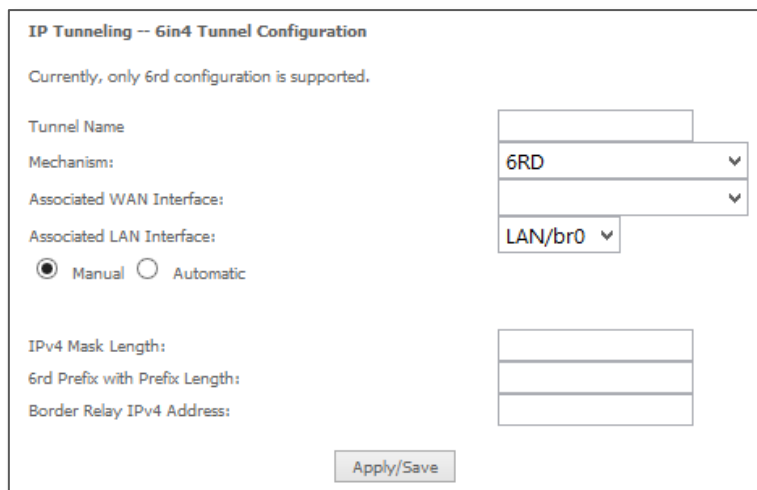
To use IPv6inIPv4 tunnelling service an active subscription to a tunnelling provider are required.



Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
<div style="text-align: center;"> Add Remove </div>							

Figure 97 – IPv6inIPv4 Tunnel list

Click the **Add** button to add a new tunnel.



IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism: 6RD ▼

Associated WAN Interface: ▼

Associated LAN Interface: LAN/br0 ▼

☒ Manual ☐ Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

Apply/Save

Figure 98 – 6in4 Tunnel configuration

IPv4inIPv6

Your ISP must support the DS-Lite IPv4inIPv6 tunnelling service, to enable this feature



Name	WAN	LAN	Dynamic	AFTR	Remove
<div style="text-align: center;"> Add Remove </div>					

Figure 99 – IPv4inIPv6 Tunnel list

Click the **Add** button to add a new tunnel.

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:

Mechanism: **DS-Lite** ▼

Associated WAN Interface: ▼

Associated LAN Interface: **LAN/br0** ▼

☒ Manual
 ☐ Automatic

Remote Address:

Apply/Save

Figure 100 – 4in6 Tunnel configuration

IPSec

Displays the IPSec tunnel connections.

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove	Edit
<div> Add New Connection Remove </div>					

Figure 101 – IPSec Tunnel Mode Connections list

IPSec Settings

IPSec Connection Name:

IP Version: **IPv4** ▼

Tunnel Mode: **ESP** ▼

Local Gateway Interface: **Select interface** ▼

Remote IPSec Gateway Address (IP or Domain):

Tunnel access from local IP addresses: **Subnet** ▼

IP Address for VPN:

Mask or Prefix Length:

Tunnel access from remote IP addresses: **Subnet** ▼

IP Address for VPN:

Mask or Prefix Length:

Key Exchange Method: **Auto(IKE)** ▼

Authentication Method: **Pre-Shared Key** ▼

Pre-Shared Key:

Perfect Forward Secrecy: **Disable** ▼

Advanced IKE Settings: **Show Advanced Settings**

Apply/Save

Figure 102 – IPsec configuration

PARAMETER	DEFINITION
IPSec Connection Name	Enter a name to identify the IPSec tunnel.
Tunnel Mode	Select the applicable IPSec tunnel mode.
Remote IPSec Gateway	Enter the IP Address of the IPSec server to connect to.
Tunnel access from Local	Select which remote addresses local IPSec connections are able to access .
IP Address from VPN	Enter the IP Address to be used locally for the IPSec tunnel.
Subnet mask for VPN	Enter the subnet mask to be used locally for the IPSec tunnel.
Tunnel Access from Remote	Select which local addresses remote IPSec connections are able to access.
IP Address for VPN	Enter the IP Address to be used on the remote end for the IPSec tunnel.
Subnet mask for VPN	Enter the subnet mask to be used on the remote end for the IPSec tunnel.
Key Exchange Method	Select the type of IPSec exchange is to be used on the IPSec tunnel.
Authentication Method	Select the applicable authentication for the IPSec tunnel.
Pre-Shared Key	Enter the pre-shared key (if applicable) to grant access to the IPSec tunnel.
Perfect Forward Secrecy	Select to use Perfect Forward Secrecy during key exchange for the IPSec tunnel.
Advanced IKE Settings	Configure advanced IKE settings for the IPSec tunnel such as the encryption method or key life time.

Table 33 – IPsec settings table

Multicast (IGMP Configuration)

The **Internet Group Management Protocol (IGMP)** is a communications protocol used by hosts and adjacent gateways on IP networks to establish multicast group memberships.

IGMP is a protocol only used on the network between a host and the gateway. It allows a host to inform the gateway whenever that host needs to join or leave a particular multicast group. IGMP provides for more efficient allocation of resources when used with online gaming and video streaming.

Multicast Precedence:
Disable
lower value, higher priority

Multicast Strict Grouping Enforcement:
Disable

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	3
Query Interval (s):	125
Query Response Interval (1/10s):	100
Robustness Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	<input checked="" type="checkbox"/>

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval (s):	125
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Groups:	10
Maximum Multicast Data Sources (for mldv2):	10
Maximum Multicast Group Members:	10
Fast Leave Enable:	<input checked="" type="checkbox"/>

Apply/Save

Figure 103 – Multicast

FIELD	DEFINITION
Default Version	The version IGMP in use by the gateway.
Query Interval	The hosts on the segment report their group membership in response to the gateway's queries. The query interval timer is also used to define the amount of time a gateway will store particular IGMP state if it does not hear any reports on the group. The query interval is the time in seconds between queries sent from the gateway to IGMP hosts.
Query Response Interval	When a host receives the query packet, it starts counting to a random value, less the maximum response time. When this time expires, the host replies with a report, provided that no other host has responded yet. This accomplishes two purposes:

FIELD	DEFINITION
	<ul style="list-style-type: none"> a) Allows controlling the amount of IGMP reports sent during a time window. b) Engages the report suppression feature, which permits a host to suppress its own report and conserve bandwidth.
Last Member Query Interval	IGMP uses this value when gateway hears IGMP Leave report. This means that at least one host wants to leave the group. After gateway receives the Leave report, it checks that the interface is not configured for IGMP Immediate Leave (single-host on the segment) and if not, it sends out an out-of-sequence query.
Robustness Value	<p>The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. You can also click the scroll arrows to select a new setting. The robustness variable should be set to a value of 2 or greater.</p> <p>The default robustness variable value is 2.</p>
Maximum Multicast Groups	The maximum number of multicast groups that the gateway can control at any one time.
Maximum Multicast Data Sources	The maximum number of data sources a multicast group can have.
Maximum Multicast Group Members	The maximum number of hosts a multicast group can have.
Fast Leave Enable	With IGMP fast-leave processing, which means that the gateway immediately removes the interface attached to a receiver upon receiving a Leave Group message from an IGMP host.

Table 34 – Multicast settings table

Wireless

WiFi 2.4GHz/WiFi 5GHz

The NL1901ACV gateway allows you to maintain separate wireless settings for both 2.4GHz and 5GHz wireless services.

Select the service you will use (or both) and separately configure them using nearly identical configuration pages:

2.4 GHz Wireless Configuration
pages

5 GHz Wireless Configuration
pages



Only the **Advanced** configuration page contains settings that are different for 5GHz wireless services.

Wireless – Basic

The Basic Wireless configuration page allows you to enable the wireless network and configure its basic settings.




Figure 104 – Wireless - Basic Configuration

The following parameters are available:

PARAMETER	DEFINITION
Enable Wireless	Select <input checked="" type="checkbox"/> Enable Wireless to activate the wireless network function.
Hide Access Point	Select <input checked="" type="checkbox"/> to hide the wireless network when an SSID scan is performed.
Clients Isolation	Select <input checked="" type="checkbox"/> to prevent clients on the wireless network being able to access each other.
Disable WMM Advertise	Select <input checked="" type="checkbox"/> to prevent the NL1901ACV advertising its WMM QoS function
Enable Multicast Forwarding (WMF)	Wireless Multicast Forwarding can reduce latency and improve throughput for wireless clients.
Max Clients	Enter the maximum number of wireless clients able to connect to the wireless network
Wireless Guest / Virtual Access Points	Select to enable a separate Wireless Guest network. For each Guest network enter the same options as are available in the top of this page for the main system wireless network.

Table 35 – Basic Wireless settings table

Click **Apply/Save** to save the new wireless configuration settings.

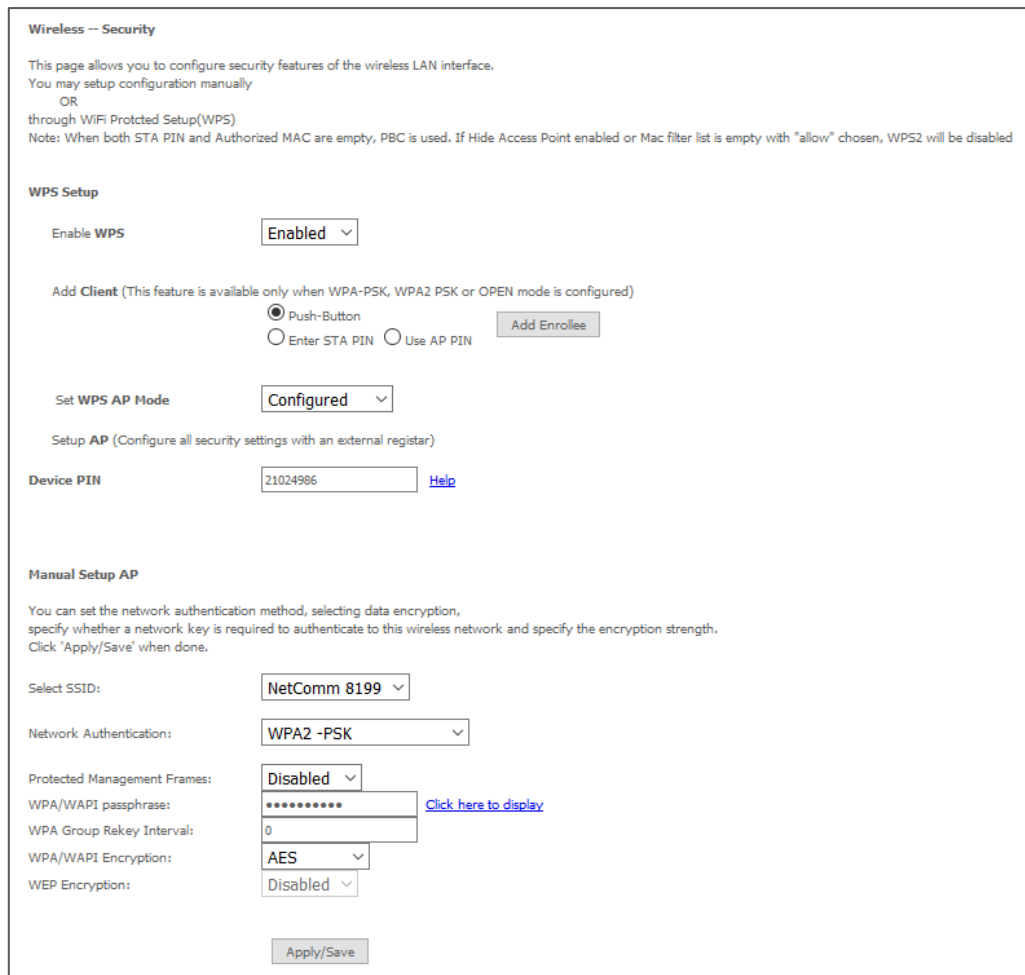


Note – Hiding the network may leads to potential connection problems, a non-broadcast network is not undetectable, and hiding a SSID is Security through obscurity

Wireless – Security

The NL1901ACV supports all encryptions within the 802.11 standard. The factory default is **WPA2-PSK**. The NL1901ACV also supports: **WPA, WPA-PSK, WPA2 or WPA2-PSK**

You can also select to disable WPS mode.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS: **Enabled**

Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
☒ Push-Button ☐ Enter STA PIN ☐ Use AP PIN [Add Enrollee](#)

Set WPS AP Mode: **Configured**

Setup AP (Configure all security settings with an external registrar)

Device PIN: **21024986** [Help](#)

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click 'Apply/Save' when done.

Select SSID: **NetComm 8199**

Network Authentication: **WPA2-PSK**

Protected Management Frames: **Disabled**

WPA/WAPI passphrase: ********* [Click here to display](#)

WPA Group Rekey Interval: **0**

WPA/WAPI Encryption: **AES**

WEP Encryption: **Disabled**

[Apply/Save](#)

Figure 105 – Wireless Security

The following parameters are available:

PARAMETER	DEFINITION
Enable WPS	Select to enable or disable the WPS function of the NL1901ACV.
Select SSID	Select the SSID to apply the security settings to.
Network Authentication	Select the Wireless security type to use with the wireless network. The default is WPA2-PSK . The NL1901ACV also supports: WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA and Mixed WPA2/WPA-PSK
WPA/WAPI passphrase	Enter the security key to use with the wireless network.
WPA Group Rekey Interval	Enter the group rekey interval. This should not need to change.
WPA/WAPI Encryption	Select the type of encryption to use on the wireless network.

PARAMETER	DEFINITION
WEP Encryption	Select to utilise WEP encryption on the wireless network connection.

Table 36 – Wireless security settings table

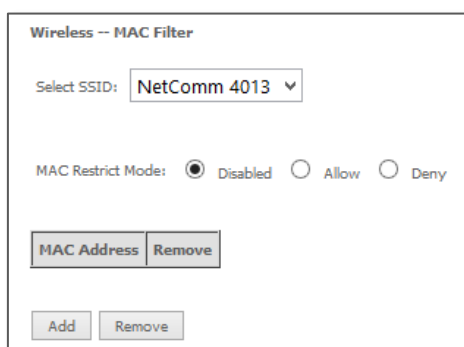


Note – WPA with TKIP and Open WEP are no longer considered secure. WPA2 with AES is the most secure option. Mixed WPA2/WPA (TKIP+AES) will provide maximum compatibility with legacy devices

Click **Apply/Save** to save the new wireless security configuration settings.

Wireless – MAC Filter

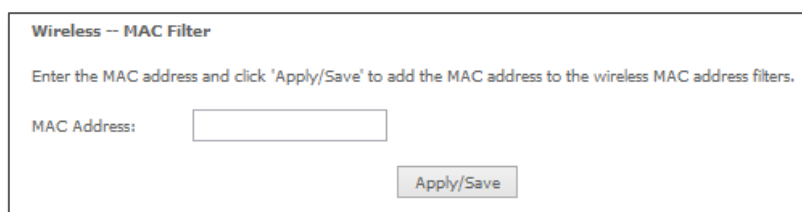
MAC Filter allows you to add or remove the MAC Address of devices which will be allowed or denied access to the wireless network. First use the **Select SSID** drop down list to select the wireless network you wish to configure, then select to either allow or deny access to the MAC addresses listed.



The screenshot shows the 'Wireless – MAC Filter' configuration window. At the top, there is a 'Select SSID:' dropdown menu with 'NetComm 4013' selected. Below this, the 'MAC Restrict Mode:' section has three radio buttons: 'Disabled' (selected), 'Allow', and 'Deny'. Underneath, there is a table with two columns: 'MAC Address' and 'Remove'. At the bottom of the window, there are two buttons: 'Add' and 'Remove'.

Figure 106 – Wireless – MAC Filter list

Click **Add** to add a MAC Address Filter.



The screenshot shows the 'Wireless – MAC Filter' configuration window. It contains a text box for 'MAC Address:' and an 'Apply/Save' button. Above the text box, there is a instruction: 'Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters.'

Figure 107 – Wireless – MAC Filter configuration

Enter the MAC Address to be filtered and click **Apply/Save** to save the new MAC Address filter settings.

To delete a MAC filter entry, click the Remove checkbox next to the selected filter entry and click Remove.

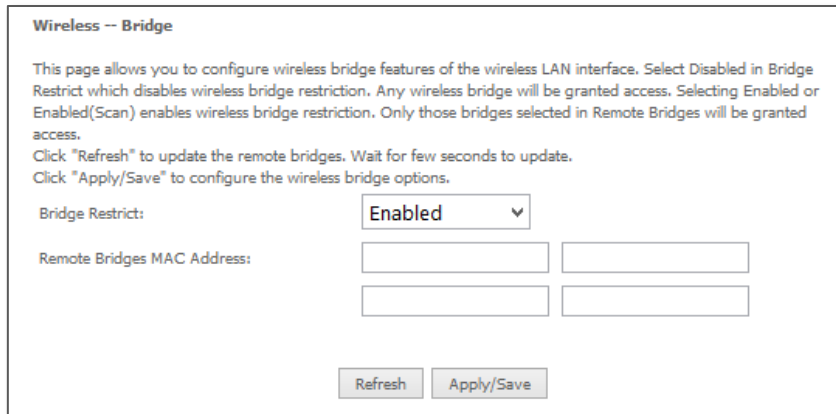
Enter MAC address in the format of aa:bb:cc:11:22:33



Note – While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC and then spoofing one's own MAC into a validated one, using MAC Filtering may lead to a false sense of security.

Wireless – Wireless Bridge (Wireless Distribution Service)

Wireless Bridge allows you to configure the gateway's access point as a Wireless Distribution Service.



The screenshot shows the 'Wireless -- Bridge' configuration page. It contains a title bar, a descriptive paragraph about the page's function, instructions for using the 'Refresh' and 'Apply/Save' buttons, a 'Bridge Restrict' dropdown menu set to 'Enabled', and four input fields for 'Remote Bridges MAC Address' arranged in a 2x2 grid. At the bottom are 'Refresh' and 'Apply/Save' buttons.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.

Click "Apply/Save" to configure the wireless bridge options.

Bridge Restrict: Enabled

Remote Bridges MAC Address:

Refresh Apply/Save

Figure 108 – Wireless Bridge page

Select the mode for the Wireless Access Point built into the NL1901ACV. You can specify which wireless networks will be allowed to connect to the NL1901ACV by using the **Bridge Restrict** option and then entering the applicable MAC Addresses of the other wireless access points.



Note – WPA/WPA2 encryption may not be compatible with other vendors, when operating in Wireless Bridge (WDS) mode.

Click **Apply/Save** to save the new wireless bridge configuration settings.

Wireless – Advanced

Advanced Wireless allows you to configure detailed wireless network settings such as the band, channel, bandwidth, transmit power, and preamble settings.

Wireless -- Advanced
 This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click 'Apply/Save' to configure the advanced wireless options.

Channel:	Auto ▼	Current: 44
Auto Channel Timer(min)	15	
802.11n/EWC:	Auto ▼	
Bandwidth:	80 MHz ▼	Current: 80MHz
Control Sideband:	Lower ▼	Current: N/A
802.11n Rate:	Auto ▼	
802.11n Protection:	Auto ▼	
Support 802.11n Client Only:	Off ▼	
RIFS Advertisement:	Off ▼	
OBSS Co-Existence:	Disable ▼	
RX Chain Power Save:	Enable ▼	Power Save status: Low Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g Rate:	6 Mbps ▼	
Multicast Rate:	Auto ▼	
Basic Rate:	Default ▼	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress Technology:	Enable ▼	
Regulatory Mode:	Disabled ▼	
Pre-Network Radar Check:	-1	
In-Network Radar Check:	-1	
TPC Mitigation(db):	0(off) ▼	
Transmit Power:	100% ▼	
WMM(Wi-Fi Multimedia):	Enabled ▼	
WMM No Acknowledgement:	Disabled ▼	
WMM APSD:	Enabled ▼	
Beamforming Transmission (BFR):	Disabled ▼	
Beamforming Reception (BFE):	Disabled ▼	
Band Steering:	Disabled ▼	
Enable Traffic Scheduler:	Disabled ▼	
Airtime Fairness:	Enabled ▼	

Apply/Save

Only available when
802.11n/EWC = 'Auto'

5 GHz only

Figure 109 – Wireless – Advanced configuration page

Click **Apply/Save** to save any changes to the wireless network settings configuration.

PARAMETER	DEFINITION
Channel	<p>Select the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly.</p> <p>This gateway supports auto channelling functionality (default setting). The Current: channel number, together with the current level of detected interference, will be displayed on the right.</p>
Auto Channel Timer (min)	<p>Specifies the interval in minutes between searches for the best wireless channel during Auto channel detection.</p> <p>It is disabled when a specific Channel is selected rather than Auto.</p>
802.11n/EWC	<p>Select 802.11n/EWC (Enhanced Wireless Consortium) functionality to be either: Disabled or Auto</p> <p>Note – When Disabled is selected the items in this table marked with '*' will be removed from the page and will not be available.</p> <p>When Auto is selected, the following ten 802.11n settings marked with '*' are enabled and displayed.</p>
Bandwidth *	<p>Select the bandwidth for the network: 20MHz, 40MHz, or 80MHz</p> <p>In high wireless activity/interference environment, reduce the bandwidth to 20MHz for greater stability.</p> <p>The Current: bandwidth will be displayed on the right.</p>
Control Sideband *	<p>If you select 20MHz in both bands you cannot select sideband and this drop down menu is disabled.</p> <p>When you select the 40MHz bandwidth in both bands and manually select a channel, the following options will appear: Lower or Upper</p> <p>When you select Lower as the control sideband, the channel is 1~7.</p> <p>When Upper, the channel is 5~11.</p> <p>The Current: control sideband (upper or lower) will be displayed on the right.</p>
802.11n Rate *	<p>Select the transmission rate for the network.</p> <p>The rate of data transmission should be set depending on the speed of your wireless network.</p> <p>You can select from a range of transmission speeds in the drop down menu, or you can select Auto to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature.</p> <p>Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client.</p> <p>The default value is Auto.</p>
802.11n Protection *	<p>The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without "speaking" at the same time.</p>
Support 802.11n Client Only *	<p>When On is selected, only stations that are configured in 802.11n mode are supported.</p> <p>Off will enable support for clients that are not 802.11n.</p>
RIFS Advertisement *	<p>Reduced Interframe Space (RIFS) is a new feature introduced in 802.11n to improve efficiency.</p>
OBSS Co-Existence *	<p>Enable OBSS (Overlapping BSS) and the gateway automatically changes the channel width from 40Mhz to 20Mhz to avoid interference with other APs and then back to 40Mhz, if possible.</p>

PARAMETER	DEFINITION
RX Chain Power Save *	When the RX Chain Power Save feature is enabled one of the receive chains will be turned off to save power. The current Power Save status : (Full Power or Low Power) will be displayed on the right.
RX Chain Power Save Quiet Time *	When RX Chain Power Save is enabled, set the number of seconds the packets per second must be below the value before the RX Chain Power Save feature activates itself.
RX Chain Power Save PPS *	When RX Chain Power Save is enabled, set the RX Chain Power Save PPS to the maximum number of packets per second that the WLAN interface should process for during RX Chain Power Save Quiet Time before the RX Chain Power Save feature activates itself.
54g Rate	Allows you to specify the maximum bandwidth of the 802.11g network.
Multicast Rate	Select the multicast transmission rate in Mbps for the network. The rate of data transmission should be set depending on the speed of your wireless network. Available settings are: Auto, 6, 9, 12, 18, 24, 36, 48, 54 Select Auto to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client. The default value is Auto.
Basic Rate	Select the basic transmission rate ability for the AP.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance. The default setting is: 2346
RTS Threshold	The RTS Threshold is the minimum size in bytes for which the Request to Send/Clear to Send (RTS/CTS) channel contention mechanism is used. The gateway sends RTS frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default setting (which is the maximum value): 2347 In a network with significant radio interference or large number of wireless devices on the same channel, reducing the RTS Threshold might help in reducing frame loss.
DTIM Interval	A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast and multicast messages. Enter a value between 1 and 255 seconds for the DTIM interval between messages.
Beacon Interval	A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is the period of time (sent with the beacon) which will elapse before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). The default (100 ms) is recommended.
XPress Technology	Select Enable to turn on this is special frame-bursting accelerating technology for IEEE802.11g. The default is Enable.

PARAMETER	DEFINITION
54g Mode (2.4 GHz and 802.11n/EWC disabled only)	For 54g mode , you can select Automatic , 802.11g Performance , or 802.11b Only . This option is only visible when 802.11n mode is set as Disabled .
54g Protection (2.4 GHz and 802.11n/EWC disabled only)	When set to Automatic , the gateway will use RTS/CTS to improve the 802.11g performance in 802.11 mixed environments. When set to Disabled , the 802.11g performance will be maximized under most conditions while the other 802.11 modes (802.11b, etc.) will be secondary. This option is only visible when 802.11n mode is set as Disabled .
Afterburner Technology (Both 2.4 GHz and 5GHz when 802.11n/EWC disabled only)	Afterburner is a 125HSM (125 High Speed Mode) speed enhancement technology for 802.11g/b.
Preamble Type (2.4 GHz and 802.11n/EWC disabled only)	If you are not using any 802.11b devices in your network, set the Preamble Type to Short for optimum performance. The Long Preamble type should be used when both 802.11g and 802.11b devices exist on your network. Preamble Type defines the length of the Cyclic Redundancy Check (CRC) block for communication between the gateway and wireless clients. The preamble consists of the Synchronization and Start Frame Delimiter (SFD) fields. The sync field is used to indicate the delivery of a frame to wireless stations, to measure frequency of the radio signal, to perform corrections if needed. The SFD at the end of the Preamble is used to mark the start of the frame.
Regulatory Mode (5 GHz only)	Select: Disabled , 802.11h or 802.11d The default is Disabled .
Pre-Network Radar check (5 GHz only)	Available only in the 802.11h Regulatory Mode, see last setting. The default is: -1
TPC Migration (db) (5 GHz only)	Select: 0(off) , 2 , 3 or 4 The default is 0(off)
Transmit Power	Select: 20% , 40% , 60% , 80% or 100% The Power level sets the strength of the wireless signal that the gateway transmits. If you live in an area where your wireless signal could overlap with other wireless networks use a lower setting in order to reduce the amount of interference. The default setting is 100% .
WMM (WiFi Multimedia)	WMM (WiFi Multimedia) maintains the priority of audio, video and voice, over other applications which are less time critical by ensuring that data from applications that require better throughput and performance are inserted in queues with higher priority. Select whether WMM is: Auto , Disabled or Enabled Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
WMM No Acknowledgement	This setting is only available when WMM (WiFi Multimedia) is set to Auto or Enabled . By default, the 'Ack Policy' for each access category is set to Disabled , meaning that an acknowledgement packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance.

PARAMETER	DEFINITION
	Select Enabled to turn off the acknowledgement request. This can be useful for Voice transmissions where speed of transmission is important and packet loss is tolerable to a certain degree.
WMM APSD	<p>This setting is only available when WMM (WiFi Multimedia) is set to Auto or Enabled.</p> <p>WMM APSD (Automatic Power Save Delivery) is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.</p> <p>Select Enabled to ensure very low power consumption.</p>
Beamforming Transmission (BFR)	Select SU (Single-User) BFR to concentrate the transmission signal at the gateway location. This results in a better signal and potentially better throughput.
Beamforming Reception (BFE)	Select SU (Single-User) BFE to concentrate the transmission signal at the gateway location.
Band Steering	Select Enabled to detect if the client has the ability to use two bands. When enabled, the less-congested 5GHz network is selected (by blocking the client's 2.4GHz network).
Enable Traffic Scheduler	Select Enabled to allow scheduling of traffic to improve efficiency and increase usable bandwidth for some types of packets by delaying other types.
Airtime Fairness	Select Enabled to allow the gateway to manage the receiving signal with other devices.

Table 37 - Wireless – Advanced configuration settings

Wireless – Station Info

This page shows the MAC address of authenticated wireless stations that are connected to the NL1901ACV and their status

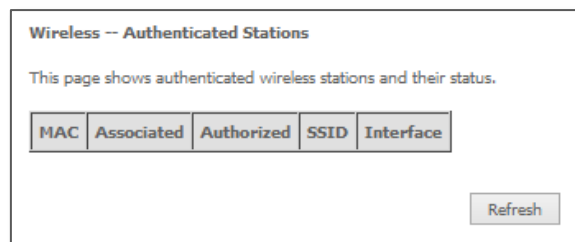


Figure 110 – Wireless – Station Info list

Voice

This section explains how to configure the VoIP settings of the NL1901ACV.

VoIP Status

The **Voice Status** page displays the registration status of your SIP accounts and the total call time of each account.

Voice -- Voice Status

Account denial will display "Disabled", registered successfully will display "Up", and unregistered will display "Down".

SIP Account	Call Time	User Accounts	Registration Status	Hook Status	Call Status
1	0:00:00	0291356598	Down	On Hook	Idle
2	0:00:00	61244100247	Down	On Hook	Idle

Active call monitoring

Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost
----------------	---------------	-----------	----------------	-----------	----------	-----------	--------------	------------------	--------------

Call history:

Index	Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost	Timestamp
1	61244100247	0294242495	10.21.95.24	103.101.168.11	2	6	out	699	333	0	Fri Oct 5 16:21:50 2018
2	0291356598	0294242495	10.21.95.24	58.96.1.2	1	2	out	661	201	0	Fri Oct 5 16:12:22 2018
3	0291356598	0294242495	10.21.95.24	58.96.1.2	1	2	out	708	153	0	Fri Oct 5 16:00:38 2018
4	0291356598	0294242495	10.21.95.24	58.96.1.2	1	2	out	572	215	0	Fri Oct 5 15:56:06 2018
5	61244100247	0294242495	10.21.95.24	103.101.168.11	2	4	out	687	365	0	Fri Oct 5 15:55:51 2018
6	61294242495	61244100247	103.101.168.11	10.21.95.24	2	16	in	1131	798	0	Fri Oct 5 15:36:58 2018
7	61294242495	61244100247	103.101.168.11	10.21.95.24	2	22	in	1313	1069	0	Fri Oct 5 15:35:34 2018
8	0294242495	0291356598	58.96.8.7	10.21.95.24	1	106	in	5584	0	0	Fri Oct 5 15:27:13 2018
9	61294242495	61244100247	103.101.168.11	10.21.95.24	2	33	in	2283	1627	0	Fri Oct 5 15:01:10 2018
10	61294242495	61244100247	103.101.168.11	10.21.95.24	2	23	in	1689	1121	0	Fri Oct 5 14:50:52 2018

Figure 111 – Voice Status page

SIP Basic Setting

The **SIP Basic Settings** page is where you enter your VoIP service settings as supplied by your VOIP service provider (VSP).

If you are unsure about a specific setting or have not been supplied information for a particular field, please contact your VoIP service provider to verify if this setting is needed or not.

Voice -- SIP Basic Setting

Bound Interface Name:

Country :

SIP local port(1-65535):

☒ Use SIP Proxy.

SIP Proxy:

SIP Proxy port:

☒ Use SIP Outbound Proxy.

SIP Outbound Proxy:

SIP Outbound Proxy port:

☒ Use SIP Registrar.

SIP Registrar:

SIP Registrar port:

☒ Use SIP Proxy2.

SIP Proxy2:

SIP Proxy2 port:

☒ Use SIP Outbound Proxy2.

SIP Outbound Proxy2:

SIP Outbound Proxy2 port:

☒ Use SIP Registrar2.

SIP Registrar2:

SIP Registrar2 port:

SIP Account	1	2
Account Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Polarity Reverse Enable	<input type="checkbox"/>	<input type="checkbox"/>
Authentication name	0291356598	61244100247
Password	*****	*****
Cid Name	0291356598	61244100247
Cid Number	0291356598	61244100247

codec--line 1	ptime[ms]	priority	enable	codec--line 2	ptime[ms]	priority	enable
G711U	20 ▾	1 (1-100)	<input checked="" type="checkbox"/>	G711U	20 ▾	1 (1-100)	<input checked="" type="checkbox"/>
G711A	20 ▾	2 (1-100)	<input checked="" type="checkbox"/>	G711A	20 ▾	2 (1-100)	<input checked="" type="checkbox"/>
G729	30 ▾	3 (1-100)	<input checked="" type="checkbox"/>	G729	30 ▾	3 (1-100)	<input checked="" type="checkbox"/>
G723_63	30 ▾	4 (1-100)	<input checked="" type="checkbox"/>	G723_63	30 ▾	4 (1-100)	<input checked="" type="checkbox"/>
G726_24	20 ▾	5 (1-100)	<input checked="" type="checkbox"/>	G726_24	20 ▾	5 (1-100)	<input checked="" type="checkbox"/>
G726_32	20 ▾	6 (1-100)	<input checked="" type="checkbox"/>	G726_32	20 ▾	6 (1-100)	<input checked="" type="checkbox"/>
G726_16	20 ▾	7 (1-100)	<input checked="" type="checkbox"/>	G726_16	20 ▾	7 (1-100)	<input checked="" type="checkbox"/>
G726_40	20 ▾	8 (1-100)	<input checked="" type="checkbox"/>	G726_40	20 ▾	8 (1-100)	<input checked="" type="checkbox"/>
G722	20 ▾	9 (1-100)	<input checked="" type="checkbox"/>	G722	20 ▾	9 (1-100)	<input checked="" type="checkbox"/>

Apply

Figure 112 – SIP Basic Settings page

The individual fields shown above on the SIP Basic Settings page are explained in the following table.

OPTION	DEFINITION
Bound Interface Name	Select the Interface that the VoIP account will use to make a connection to the VoIP Service Provider.
SIP Local Port	Set the SIP local port of the gateway, the default value is 5060. SIP local port is the SIP UA (user agent) port.
Use SIP Proxy	<p>Select <input checked="" type="checkbox"/> Use SIP Proxy if your DSL gateway uses a SIP proxy. SIP proxy allows other parties to call DSL gateway through it. When it is selected, the following fields appear.</p> <ul style="list-style-type: none"> • SIP Proxy – Enter the IP address of the proxy. • SIP Proxy port – Enter the port that this proxy is listening on. By default, the port value is 5060.
Use SIP Outbound Proxy	<p>Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and it is the only way to let SIP traffic pass from the internal network to the Internet.</p> <p>When it is selected, the following fields appear:</p> <ul style="list-style-type: none"> • SIP Proxy – Enter the IP address of the outbound proxy. • SIP Proxy port – Enter the port that this outbound proxy is listening on. By default, the port value is 5060.
Use SIP Registrar	<p>Select this option if required by your VoIP Service Provider. Enter the SIP Proxy Domain Name and SIP Proxy Port which is typically 5060.</p> <p>When it is selected, the following fields appear:</p> <ul style="list-style-type: none"> • SIP Registrar– Enter the IP address of the SIP registrar. • SIP Registrar port – Enter the port that the SIP registrar is listening on. By default, the port value is 5060.
Account Enabled	If it is unselected, the corresponding account is disabled, you cannot use it to initiate or accept any call.
Polarity Reverse Enable	Enable or disable this function.
Authentication name	Set the user name of authentication.
Password	Set the password of authentication.
Cid Name	User name. It is the Display Name.
Cid Number	Set the caller number. It must be a number of 0~9 .
ptime	You can use it to set the packetization time (PT). The PT is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. If selecting 10 milliseconds, packets improve the voice quality. Because of the packet loss, less information is lost, but more loads on the network traffic.
Priority	The priority of codec is declined from up to down. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G723 is a codec that uses compression, therefore, it is good for use where the bandwidth is limited but its voice quality is not good as other codecs, such as the G711. If you specify none of the codecs, using the default value showed in the above figure, the DSL gateway chooses the codec automatically.

Table 38 – SIP settings table

After entering your VoIP settings press the **Apply** button.

SIP Advanced Setting

The **SIP Advanced Setting** page allows you to configure settings that your VoIP service provider has enabled on your SIP account and if you have the appropriate call features and other functionality on your cordless or corded phone handsets.

Line

1

2

Call waiting

☒

☒

Unconditionally Call forwarding number

Busy Call forwarding number

No Answer Call forwarding number

Options Time

0

0

Forward unconditionally

☒

☒

Forward on "busy"

☒

☒

Forward on "no answer"

☒

☒

HWI

☐

☐

Anonymous call blocking

☒

☒

Anonymous calling

☒

☒

Anonymous calling mode

Display anonymous

Display anonymous

DND

☐

☐

Enable Call Return

☐

☐

Call Transfer

☒

☒

Call conference

☐

☐

Warm Line

☒

☒

Warm Line URI

Warm Line Delay Timer

10

10

==Fax Setting==

Fax Negotiate Mode:

Auto_switch

Bypass Codec:

G711_A

☐ Enable T38 redundancy support

☐ Enable vbd redundancy support

==Settings==

☒ Enable VAD support

VAD mode in signal:

None

☐ Enable RTP Flow Ctrl

☒ Enable Echo Cancellation

☐ Enable # To ASCII

==SIP Timer Setting==

Registration Expire Timeout:

3600

Session Expire Timeout:

1800

Min Session Expire Times:

90

(need >= 90s)

==Digitmap Setting==

000|[*#]X[0-9*].#|*XX|*X[0-9*].#|*X[0-9*].#|00[1-9]xx.t|014XXXXXXXX|016XXXXX
XX|0192X|0198XXXXXXXX|0[23478]XXXXXXXX|0500XXXXXXXX|11XX|123X|124XX|1251XX|1252XX
X|1255X|1258XXX|1271X|130XXXXXXXX|1802XXX|189XX|1[8-9]XXXXXXXX|
[2-9]XXXXXXXX|13[1-9]XXX

Voip Dialplan Setting:

==Qos Setting==

DSCP for SIP:

DEFAULT (000000)

DSCP for RTP:

DEFAULT (000000)

==Payload Setting==

RFC2198 Payload Value:

125

(range 97~127)

Dtmf Relay setting:

InBand

==Call ID Setting==

Caller ID send Delay Time:

600

(range 500~1500ms)

Caller ID Message Type:

FSK_MDMF

FSK modulation Mode:

BellcoreGen

==Transport Setting==

SIP Transport protocol:

UDP

==SIP Extends==

PRACK (100rel):

SUPPORTED

==Service Offer Setting==

Complementary business models:

Local model

Apply

Figure 113 – Voice- SIP Advanced settings

OPTION	DEFINITION
Line	Displays the phone port you want to configure, the NL1901ACV supports two phone lines.
Call Waiting	Select this option for your phone if your VoIP Service Provider has enabled Call Waiting on your SIP account.
Unconditionally Call forwarding number	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Busy Call Forwarding Number	Enter the phone number to forward a call to if it arrives while the line is busy.
No Answer Call forwarding number	Enter the phone number to forward a call to if the call is not answered.
Forward On "busy"	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Forward On "No Answer"	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
MWI (Message Waiting Indicator)	Select this option if your VoIP Service Provider has enabled MWI (Message Waiting Indicator) on your SIP account and you wish to use this feature.
Anonymous Call Blocking	Select this option if your VoIP Service Provider has enabled Anonymous Call Blocking on your SIP account and you wish to use this feature.
Anonymous Calling	Select this option if your VoIP Service Provider has enabled Anonymous Calling on your SIP account and you wish to use this feature.
Anonymous calling mode	When set to Display anonymous, the gateway hides your caller ID. When set to All anonymous, the gateway hides both caller ID and the SIP URL of the originating call.
DND (Do Not Disturb)	Select this option if your VoIP Service Provider has enabled DND (Do Not Disturb) on your SIP account and you wish to use this feature.
Enable Call Return	Select this if your VoIP Service Provider supports Call Return on your SIP account and you wish to use this feature.
Call Transfer	Select this if your VoIP Service Provider supports Call Transfer on your SIP account and you wish to use this feature.
Call conference	Select this if your VoIP Service Provider supports Conference Calling on your SIP account and you wish to use this feature.
Warm Line	Select this if your VoIP Service Provider supports Warm Line functionality on your SIP account and you wish to use this feature.
Warm Line URI	Enter the Uniform Resource Identifier (URI) of the destination number.
Warm Line Delay Timer	Enter length of time in seconds before a warm line dials the Warm Line URI, see previous.

OPTION	DEFINITION
<u>Fax Setting</u>	
Enable T38 Redundancy Support	Select this function if you wish to send or receive faxes via VoIP and have a fax machine capable of using the T38 fax over VoIP protocol.
Enable VBD redundancy support	Select this checkbox to use the feature.
<u>Settings</u>	
Enable VAD support	Enables the Voice Activity Detection function of the gateway. When enabled, no data is transmitted during periods of silence or low volume, reducing the data usage.
Enable RTCP Flow Control	Select this checkbox to use the feature.
Enable Echo Cancellation	Select this checkbox to use the feature.
Enable # To ASCII	Select this checkbox to use the feature.
<u>SIP Timer Setting</u>	
Registration Expire Timeout	Enter the registration expire timeout.
Session Expire Time	The interval of dialog refreshing time.
Min Session Expire Time	The minimum interval of dialog refreshing time.
<u>Digitmap Setting</u>	
VoIP DialPlan Setting	Set the VoIP dial plan. If user-dialled number matches it, the number is processed by the VoIP gateway immediately.
<u>QoS Setting</u>	
DSCP for SIP	Set the DSCP QoS tagging for Session Initiation Protocol. You can select it from the drop-down list.
DSCP for RTP	Set the DSCP QoS tagging for Real-time Transport Protocol. You can select it from the drop-down list.
Ethernet Priority Mark	
<u>Payload Setting</u>	
RFC2198 Payload Value	Enter the RFC2198 payload value, the valid range is 96 ~ 127.
Dtmf Relay Setting	Set DTMF transmit method, which can be one of the following: SIP Info – Use SIP INFO message to transmit DTMF digits. RFC2833 – Use RTP packet to encapsulate DTMF events, as specified in RFC 2833. InBand – DTMF events are mixed with user voice in RTP packet.
<u>Call ID Setting</u>	
Caller ID send Delay Time	Set the delay time in milliseconds between 500 to 15000ms.
Caller ID Message Type	Select the Caller ID Message Type for your area: FSK_SDMF , FSK_MDMF or DTMF
FSK modulation Mode	Select your preferred Frequency-shift keying (FSK) mode: BellcoreGen , V23Gen or V23UK

OPTION	DEFINITION
<i>Transport Setting</i>	
SIP Transport Protocol	Select the transport protocol to use for SIP signalling. Note that your SIP proxy and registrar will need to support the protocol you select.
<i>SIP Extends</i>	
PRACK (100rel)	
Agent Header	
<i>Service Offer Settings</i>	
Complementary business models	

Table 39 – VoIP – Advanced – Service Provider settings

Configuring a VoIP dial plan

The gateway comes with a default dial plan suitable for use in Australia. The dial plan tells the gateway to dial a number immediately when a string of numbers entered on a connected handset matches a string in the dial plan. For example, the string 13[1-9]XXX allows the gateway to recognize six digit “13 numbers” allowing customers to call a business for the price of a local call anywhere in Australia. The reason it is configured as 13[1-9]XXX is because 13 numbers cannot begin with a 0 after the 13 while the last 3 digits may be any numeric digit.

You can configure the dial plan to match any string you like. Below are some rules for configuring a dial plan:

- Separate strings with a | (pipe) character.
- Use the letter X to define any single numeric digit.
- Use square brackets to specify ranges or subsets, for example:
 - [1-9] allows any digit from 1 to 9.
 - [247] allows either 2 or 4 or 7.
 - Combine ranges with other keys, for example, [247-9*#] means 2 or 4 or 7 or 8 or 9 or * or #.

Dial plan syntax

DIAL PLAN SYNTAX		
TO SPECIFY A...	ENTER	RESULT
New dial string	(Pipe)	Separates dial strings
Digit	0 1 2 3 4 5 6 7 8 9	Identifies a specific digit (do not use #)
Range	[digit-digit]	Identifies any digit dialled that is included in the range
Wild card	X	X matches any single digit that is dialled
Timer	.t (dot t)	Indicates that an additional time out period of 4 seconds should take place before automatic dialling starts

Table 40 – Dial Plan Syntax table

Dial plan example: Australia Dial Plan

```
000|[*#]X[0-9*]|*#X[0-9*]|00[1-9]XX.t|014XXXXXXXX|016XXXXXXXX|0192X|0198XXXXXXXX|0[23478]XXXXXXXX|0500XXXXXXXX|11XX|123X|124XX|1251XX|1252XXX|1255X|1258XXX|1271X|130XXXXXXXX|13[1-9]XXX|1802XXX|189XX|1[8-9]XXXXXXXX|[2-9]XXXXXXXX
```

000 = Australia Emergency Call Service

0011*t = International number (After 0011 the gateway allows entry of arbitrary digits then and dials out after 4 seconds from the entry of the last digit.)(Note: Please ensure your VoIP provider supports international numbers for the country you are dialling.)

0[23478]XXXXXXXX = Landline numbers with area code 02,03,04,07,08 +XXXX XXXX and Mobile numbers with 04XXXXXXXXXX)

1[8-9]XXXXXXXX = 1800 and 1900 free call numbers

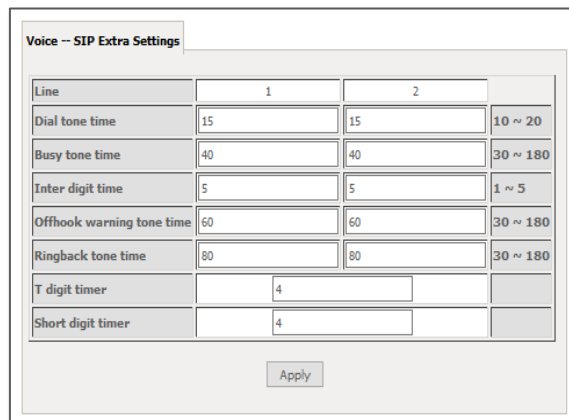
130XXXXXXXX = 1300 business numbers

13[1-9]XXX = 13 business numbers

[2-9]XXXXXXXX = Landline numbers without area code

SIP Extra Setting

This page displays additional settings related to the SIP service.



Line	1	2	
Dial tone time	15	15	10 ~ 20
Busy tone time	40	40	30 ~ 180
Inter digit time	5	5	1 ~ 5
Offhook warning tone time	50	60	30 ~ 180
Ringback tone time	80	80	30 ~ 180
T digit timer	4		
Short digit timer	4		

Apply

Figure 114 – SIP Extra Setting page

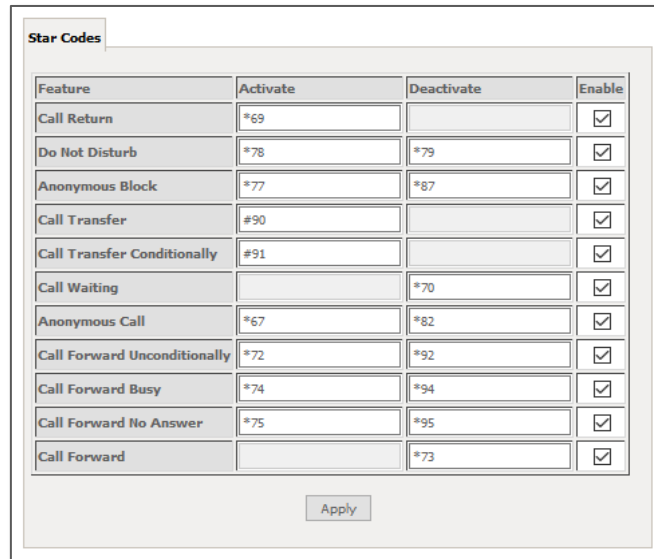
PARAMETER	DEFINITION
Dial tone time	Set the Dial tone duration.
Busy tone time	Set the Busy tone duration.
Inter digit time	Set the timing between digits. The valid range is 1 ~ 5.
Off hook warning tone time	Set the Off-hook warning tone duration.
Ringback tone time	Set the Ring back tone duration.

Table 41 – SIP Extra Settings table

SIP Star Code Setting

The SIP Star Code Setting page provides you with the ability to configure the codes used to active and deactivate call features such as call forwarding and call waiting.

Please consult your VoIP provider if SIP Star Code is supported on SIP side.



Star Codes

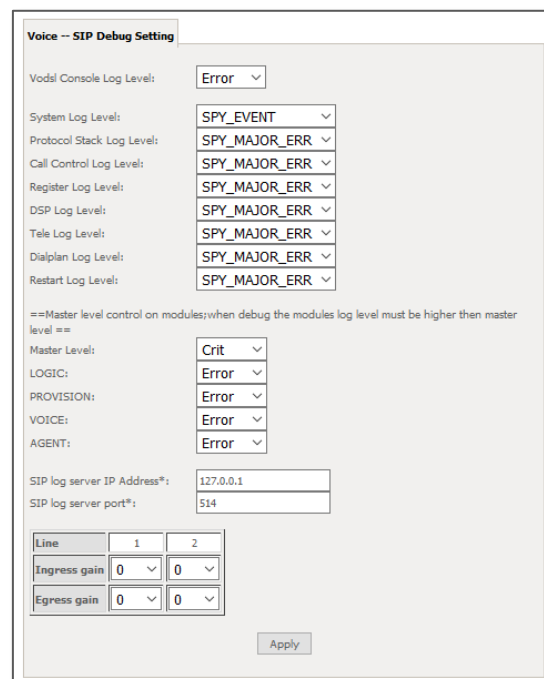
Feature	Activate	Deactivate	Enable
Call Return	*69		<input checked="" type="checkbox"/>
Do Not Disturb	*78	*79	<input checked="" type="checkbox"/>
Anonymous Block	*77	*87	<input checked="" type="checkbox"/>
Call Transfer	*90		<input checked="" type="checkbox"/>
Call Transfer Conditionally	*91		<input checked="" type="checkbox"/>
Call Waiting		*70	<input checked="" type="checkbox"/>
Anonymous Call	*67	*82	<input checked="" type="checkbox"/>
Call Forward Unconditionally	*72	*92	<input checked="" type="checkbox"/>
Call Forward Busy	*74	*94	<input checked="" type="checkbox"/>
Call Forward No Answer	*75	*95	<input checked="" type="checkbox"/>
Call Forward		*73	<input checked="" type="checkbox"/>

Apply

Figure 115 – SIP Star Code Setting page

SIP Debug Setting

This page allows you to configure various settings regarding the logging levels of the SIP service.



Voice -- SIP Debug Setting

Vodsi Console Log Level:

System Log Level:

Protocol Stack Log Level:

Call Control Log Level:

Register Log Level:

DSP Log Level:

Tele Log Level:

Dialplan Log Level:

Restart Log Level:

==Master level control on modules;when debug the modules log level must be higher then master level ==

Master Level:

LOGIC:

PROVISION:

VOICE:

AGENT:

SIP log server IP Address*:

SIP log server port*:

Line	1	2
Ingress gain	<input type="text" value="0"/>	<input type="text" value="0"/>
Egress gain	<input type="text" value="0"/>	<input type="text" value="0"/>

Apply

Figure 116 – SIP Debug Settings page

OPTION	DEFINITION
SIP Log Server IP Address	Enter the Log Server IP address where the SIP Log data for the gateway will be sent to.
SIP Log Server port	Enter the port to be used for transmitting the SIP Log data.
Ingress Gain	Setting allow control of Speaker volume on handset.
Egress Gain	Settings allow control of Microphone volume on handset.

Table 42 – SIP Debug Settings table

VoIP Functionality

This section describes how to use the VoIP function of the DSL gateway in more detail. Some features involve 2 or 3 parties. In those cases, note that all 3 parties have to be successfully registered.

Registering

Before using any VoIP functions, the DSL gateway has to register itself to a registrar.

The DSL gateway also has to be configured with a proxy, which relays VoIP signalling to the next hop. In fact, many implementations integrate these two into one server, so in many case registrar and proxy refer to the same IP.

- 1 Select the right interface to use for registering, depending on where proxy/registrar resides. If using a WAN link, ensure that it is already up.
- 2 Select ☒ **Use SIP Registrar**, and fill in the IP address and port with the correct value.
- 3 Fill the extension information: **Authentication name**, **Password**, **Cid Name** and **Cid Number**.
- 4 Click **Apply** to take the settings into effect.
- 5 **TEL** indicator of VoIP service should be on, indicating that SIP client is successfully registered.

Placing a Call

This section describes how to place a basic VoIP call.

- 1 Pick up the receiver on the phone.
- 2 Hear the dial-tone. Dial the extension of remote party.
- 3 To end the dialling, wait for digit timeout, or just press **#** immediately.
- 4 After the remote party answers the call, you are in voice connection.

Anonymous call

Anonymous call does not send the caller ID to the remote party. This is useful if you do not want others know who you are. Check with your VoIP Provider if your service supports hidden caller ID.

- 1 Enable **Anonymous calling** in the **Voice--SIP Advanced Setting** page.
- 2 Pick up the receiver on the phone.
- 3 Dial ***67** to enable anonymous call.
- 4 Hook on the receiver, and dial another extension as you like. Now your caller ID information is blocked.

Do Not Disturb (DND)

If DND is enabled, all incoming calls are rejected. DND is useful if you do not want others to disturb you. Check with your VoIP Provider if your service supports DND.

- 1 Enable **DND** in the **Voice--SIP Advanced Setting** page.
- 2 Pick up the receiver on the phone.
- 3 Dial ***78** to enable **DND**.
- 4 Hook on the phone. Now your phone rejects all incoming calls.
- 5 Hook off again to disable the DND.

Call Return

For incoming calls, the DSL gateway remembers the number of calling party. Check with your VoIP Provider if your service supports Call returns. You cannot call return, if the caller has hidden caller ID.

- 1 Enable **Call Return** ☒ in the **Voice--SIP Advanced Setting** page.
- 2 Press ***69** to return a call.
- 3 Now you can make the call as if you have dialled the whole number.

Call Hold

Call hold enable you to put a call to a pending state, and pick it up in future. Check with your VoIP Provider if your service supports Call Hold.

- 1 Assuming you are in a voice connection, you can press **FLASH** to hold current call.
- 2 Now you can call another party, or press **FLASH** again to return to first call.

Call Waiting

Call waiting allows third party to call in when you are in a voice connection. Check with your VoIP Provider if your service supports Call Waiting.

- 1 Enable **Call waiting** in the **Voice--SIP Advanced Setting** page.
- 2 Pick up the phone attached to the DSL gateway.
- 3 Assuming you are in a voice connection. When another call comes in, the DSL gateway streams a call waiting tone to your phone, indicating another call is available.
- 4 Press **FLASH** to switch to this call and the initial call put to hold automatically.
- 5 Press **FLASH** multi-times to switch between these two calls back and forth.

Call Transfer

Call transfer, transfers the current call to a third party blindly, regardless of whether the transfer is successfully or not. Check with your VoIP Provider if your service supports Call transfer.

- 1 Assume you have already been in a voice connection.
- 2 Press **FLASH** to hold the first party.
- 3 Dial **#90** + third party number.
- 4 Before the third party answering the call, hook on your phone.

- 5 Now the first party takes over the call and he is in connection with the third party.

Consultative Transfer

Consultative transfer lets the third party answer the transferred call, and then hook on the transferring party. It is more gentle than call transfer. Check with your VoIP Provider if your service supports Consultative Transfer.

- 1 Assume you have already been in a voice connection with a first party.
- 2 Press **FLASH** to hold the first party.
- 3 Dial **#91** + third party number.
- 4 After the third party answering the call, hook on your phone.
- 5 Now the first party takes over the call and he is in connection with the third party.

Call Forwarding No Answer

If this feature enabled, incoming calls are forwarded to third party when you does answer them. It involves in two steps: setting the forwarding number and enable the feature. Check with your VoIP Provider if your service supports Call Forwarding.

- 1 Enable Forward on "no answer" in the **Voice--SIP Advanced Setting** page.
- 2 When our phone does not answer the incoming call, the call is forwarded.

Call Forwarding Busy

If this feature enabled, incoming calls will be forwarded to third party when you busy. It involves two steps: setting the forwarding number and enable the feature. Check with your VoIP Provider if your service supports Call Forwarding

- 1 Enter a **Busy Call forwarding number** and enable **Forward on "busy"** ☒ in the **Voice--SIP Advanced Setting** page.
- 2 When our phone is busy, this call can be forwarded.

Call Forwarding All

If this feature enabled, incoming calls are forwarded to third party without any reason. It involves in two steps: setting the forwarding number and enable the feature. Check with your VoIP Provider if your service supports Call Forwarding

- 1 Enter an **Unconditionally Call forwarding number** and enable **Forward Unconditionally** ☒ in the **Voice--SIP Advanced Setting** page.
- 2 All incoming calls are forwarded to the third party.

Three-Way Conference

Three-way conference enables you to invite a third party to a call, and every person in the conference is able to hear others' voice. Check with your VoIP Provider if your service supports Conference call.

- 1 Assume you are in connection with a first party.
- 2 Press **FLASH** to put the first party on-hold.
- 3 Dial a third party.
- 4 After the third party answers the call, press **FLASH** again to invite the first party.

5 Now all three parties are in a three-way conference.

T.38 Faxing

To enable T.38 faxing, select ☒ **Enable T.38 support** on the **Voice--SIP Advanced Setting** page. After that, connect a fax machine to a FXS port of the DSL gateway. Now you can use it as a normal phone, and it is able to send or receive fax to or from other fax machines on the VoIP network.

In the initial setup, faxing behaves like a normal call. After the DSL gateway detects the fax tone, it switches to T.38 mode, and uses it as the transmit approach.

Check with your VoIP Provider if your service supports T.38 Faxing.

Pass-Through Faxing

If T.38 support is disabled, faxing uses normal voice codec as its coding approach. Therefore, this mode is more like normal phone calls.

Diagnostics

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider. You may diagnose the connection by clicking the **Test** button or click the **Test With OAM F4** button. If the test continues to fail, click **Help** and follow the troubleshooting procedures.



Note – Your Internet service provider must support diagnostics features in order for correct DSL diagnostics results.

Diagnostics – Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status:

- 1 Click on the **Help** link and follow the troubleshooting procedures in the Help screen that appears.
- 2 Now click **Rerun Diagnostic Tests** at the bottom of the screen to re-test and confirm the error.
- 3 If the test continues to fail, contact Technical Support.

ETH WAN Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

eth0 Connection Test:	PASS	Help
eth1 Connection Test:	FAIL	Help
eth2 Connection Test:	FAIL	Help
eth3 Connection Test:	FAIL	Help
Wireless Connection Test:	PASS	Help

Test the connection to your DSL service provider

xDSL Synchronization Test:	FAIL	Help
ATM OAM F5 segment ping Test:	FAIL	Help
ATM OAM F5 end-to-end ping Test:	FAIL	Help

Test the connection to your Internet service provider

Ping default gateway Test:	PASS	Help
Ping primary Domain Name Server Test:	FAIL	Help

Next Connection

Test

Test With OAM F4

Figure 117 – Diagnostics – ETH WAN Diagnostic test results

FIELD	DESCRIPTION
Title	The title indicates what service is being tested for the displayed test results. Types include ETH WAN Diagnostics , Mobile Diagnostics , xDSL Diagnostics , etc.
LAN# Connection	PASS – Indicates the Ethernet connection to your computer is connected to the numbered LAN port of the gateway. FAIL – Indicates that the gateway does not detect the Ethernet interface of your computer.
Wireless Connection Test	PASS – Indicates that the wireless interface from your computer is connected to the LAN port of the gateway.

FIELD	DESCRIPTION
	FAIL – Indicates that the gateway does not detect the wireless interface.
Help	Click the Help link for more details and for additional Troubleshooting advice.

Table 43 – Connection to LAN diagnostic test result table

FIELD	DESCRIPTION
xDSL Synchronization Test	PASS – Indicates the DSL modem has detected a DSL signal from the telephone company. FAIL – Indicates that the DSL modem does not detect a signal from the telephone company's DSL network.
ATM OAM F5 segment ping test	PASS – Indicates that the DSL modem can communicate with the DSL provider network. FAIL – Indicates that the DSL modem may not be able to communicate with the DSL provider network.
ATM OAM F5 end-to-end ping test	PASS – Indicates that the DSL modem can communicate with the DSL provider network. FAIL – Indicates that the DSL modem may not be able to communicate with the DSL provider network.
Help	Click the Help link for more details and for additional Troubleshooting advice.

Table 44 – Connection to DSL service diagnostic test result table

FIELD	DESCRIPTION
Ping default gateway Test	PASS – Indicates that the DSL modem can communicate with the first entry point to the network. It is usually the IP address of the ISP local router.. FAIL – Indicates that the DSL modem was unable to communicate with the first entry point on the network.
Ping primary Domain Name Server Test	PASS – Indicates that the DSL modem can communicate with the primary Domain Name Server (DNS). FAIL – that the DSL modem was unable to communicate the primary Domain Name Server (DNS).
Help	Click the Help link for more details and for additional Troubleshooting advice.

Table 45 – Connection to ISP diagnostic test result table

Diagnostics – Ethernet OAM

The Ethernet OAM page provides administrators with operation, administration and management features.

Ethernet Link OAM (802.3ah)

☒ Enabled

 WAN Interface:

 OAM ID: (positive integer)

☐ Auto Event

☐ Variable Retrieval

☐ Link Events

☐ Remote Loopback

☐ Active Mode

Ethernet Service OAM (802.1ag / Y.1731)

☒ Enabled ☒ 802.1ag ☐ Y.1731

 WAN Interface:

 MD Level: [0-7]

 MD Name: [e.g. Broadcom]

 MA ID: [e.g. BRCM]

 Local MEP ID: [1-8191]

 Local MEP VLAN ID: [1-4094] (-1 means no VLAN tag)

☐ CCM Transmission

 Remote MEP ID: [1-8191] (-1 means no Remote MEP)

Loopback and Linktrace Test

 Target MAC: [e.g. 02:10:18:aa:bb:cc]

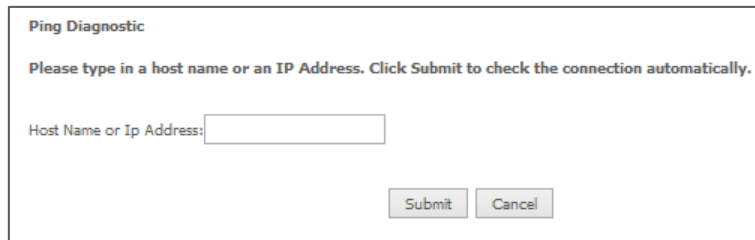
 Linktrace TTL: [1-255] (-1 means no max hop limit)

Loopback Result:	N/A			
Linktrace Result:	N/A			

Figure 118 – Diagnostics – Ethernet OAM

Diagnostics – Ping

The ping test page lets you ping a remote IP address or hostname in order to test the connection.



Ping Diagnostic

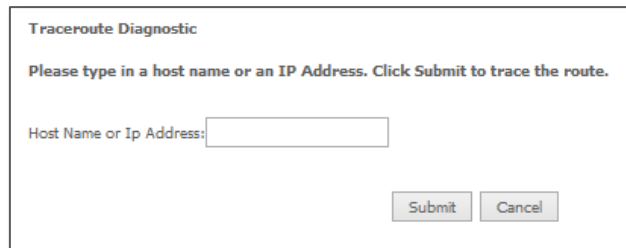
Please type in a host name or an IP Address. Click Submit to check the connection automatically.

Host Name or Ip Address:

Figure 119 – Ping IP address

Diagnostics – Traceroute

The Traceroute page lets you perform a trace route to a remote IP address or host name to ensure that the correct interface is used for routing.



Traceroute Diagnostic

Please type in a host name or an IP Address. Click Submit to trace the route.

Host Name or Ip Address:

Figure 120 – Diagnostics – Traceroute page

Diagnostics – Start/Stop DSL

This page lets you stop or start the DSL service for troubleshooting purposes.



Your DSL connection is down. Verify that your Gateway is correctly connected to your phone line. If the problem persists, check your documentation.

Start/Stop DSL

This page enables you to start or stop your DSL line.

Your DSL connection is Down, it seems the phone line is not connected.

Figure 121 – Diagnostics – Start/Stop DSL page

Management

Management – Settings

The Settings screens allow you to back up, retrieve and restore the default settings of your NL1901ACV gateway. It also provides a function for you to easily update your gateway's firmware.

Backup

The following screen appears when Backup is selected. Click the **Backup Settings** button to save the current configuration settings.

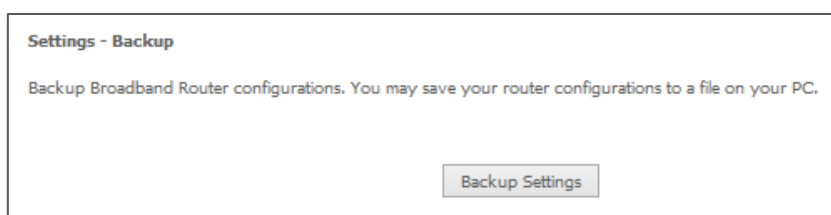


Figure 122 – Settings – Backup page

The backup file called **backupsettings (version no.) .conf** will be saved to your browser's designated download folder on your PC.



Note – Successive backup files will be numbered sequentially with their version number in brackets, e.g. **backupsettings (5) .conf**

Update Settings

The following screen appears when selecting **Update** from the **Management > Settings** submenu.

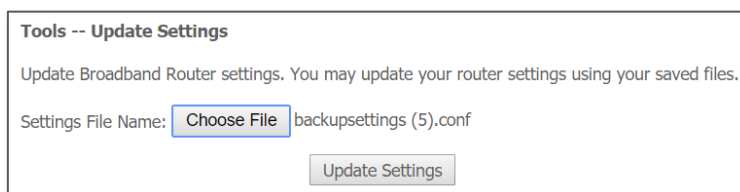


Figure 123 – Settings – Update Settings page

Use the **Choose File** button to locate a previously saved configuration backup file having the **.conf** file extension, for example: **backupsettings (5) .conf**

Click on the **Update Settings** button to upload the selected file.

Allow up to five minutes for system updates and reboot. Then log in using the **Sign in** page.

Factory Reset

The following screen appears when selecting **Factory Reset** from the **Management > Settings** submenu.

Click the **Restore Default Settings** button to remove all user defined settings and then restore the gateway's factory default firmware settings.

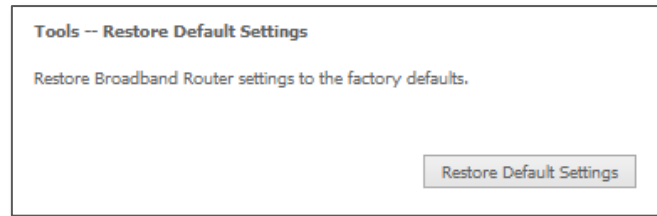


Figure 124 – Settings – Factory Reset page

Allow up to five minutes for system reset and automatic reboot. Then log in using the **Sign in** page.

Management – System Log

The System log page allows you to view the log of the gateway and configure the logging level also. To view the system log, click the **View System Log** button.

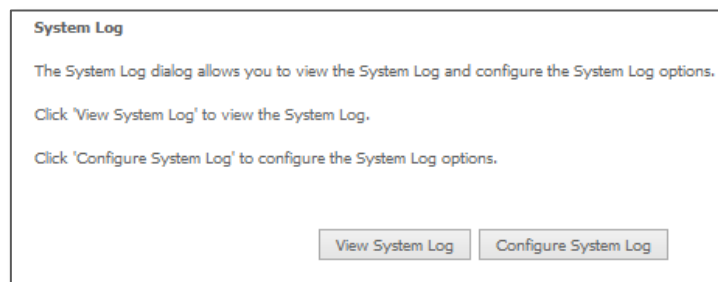


Figure 125 – Management – View System Log

Configure Log Output

To configure the system log's content and destination click the **Configure System Log** button.

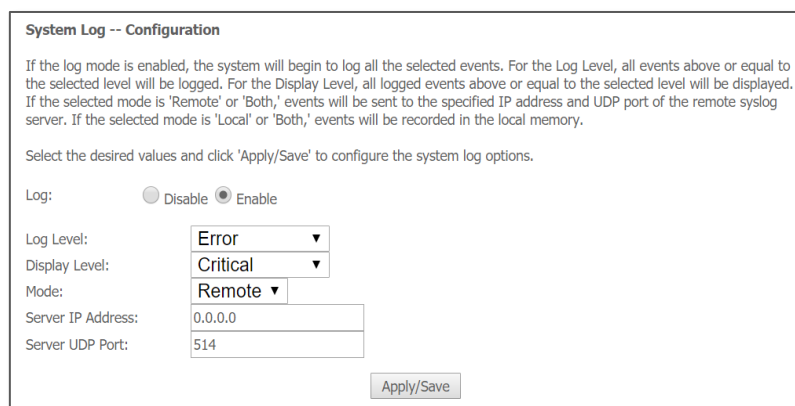
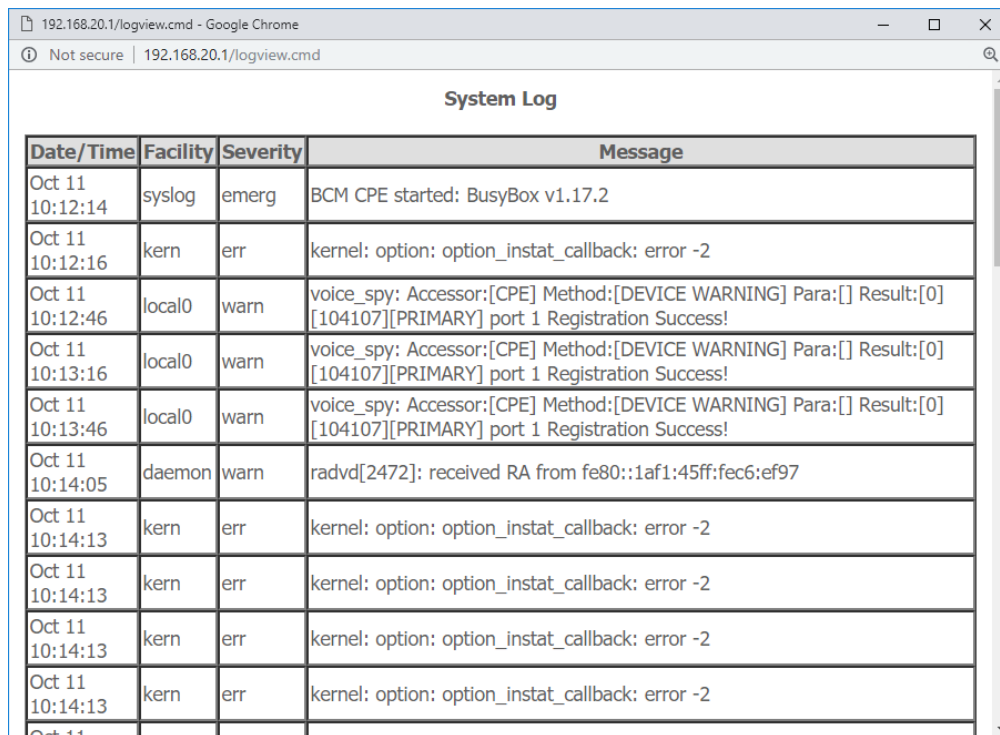


Figure 126 – Management – Configure System Log

ITEM	DESCRIPTION	
Log	Select <input checked="" type="radio"/> Disable to turn off all system logging. Select <input type="radio"/> Enable to begin logging according to the settings made on this page.	
Log Level	This setting controls the types and amount of data that is saved to the log file. The event types listed at right are listed in increasing (bottom to top) levels of importance. Select a level to log <u>that type</u> of event <u>and all</u> types of events <u>above</u> that level.	<ul style="list-style-type: none">• Emergency• Alert• Critical• Error• Warning• Notice• Informational• Debugging
Display Level	This setting controls the types and amount of data that is displayed when the View System Log button is pressed, see next section. The event type display filter is exactly the same as the Log Level event type controls: Select a level to display <u>that type</u> of event <u>and all</u> types of events <u>above</u> that level. The event types are listed in increasing levels of importance	
Mode	This setting determines where the log file, defined in Log Level , is saved to: Local – Saves the log data locally in the internal memory of the NI1901ACV gateway. Remote – Exports the log data to a remote syslog server, e.g. for remote monitoring/systems analysis, etc.. Both – Retains the data both locally and on a remote syslog server.	
Server IP Address	For Remote or Both modes (see previous item) enter the IP Address of the remote syslog server that the data will be sent to.	
Server UDP Port	For Remote or Both modes (see Mode item, above) enter the UDP Port that will be used to transmit the data to the remote syslog server.	
Apply/Save button	Click to generate a log according to the Log and Display Level settings and save or send it to the destination selected in the Mode drop down list.	

View System Log

After defining the range of its content with the **Display Level** settings of the **System Log – Configuration** page, click the **View System Log** button on the **System Log** page to open the **System Log** in its own window:



Date/Time	Facility	Severity	Message
Oct 11 10:12:14	syslog	emerg	BCM CPE started: BusyBox v1.17.2
Oct 11 10:12:16	kern	err	kernel: option: option_instat_callback: error -2
Oct 11 10:12:46	local0	warn	voice_spy: Accessor:[CPE] Method:[DEVICE WARNING] Para:[] Result:[0] [104107][PRIMARY] port 1 Registration Success!
Oct 11 10:13:16	local0	warn	voice_spy: Accessor:[CPE] Method:[DEVICE WARNING] Para:[] Result:[0] [104107][PRIMARY] port 1 Registration Success!
Oct 11 10:13:46	local0	warn	voice_spy: Accessor:[CPE] Method:[DEVICE WARNING] Para:[] Result:[0] [104107][PRIMARY] port 1 Registration Success!
Oct 11 10:14:05	daemon	warn	radvd[2472]: received RA from fe80::1af1:45ff:fec6:ef97
Oct 11 10:14:13	kern	err	kernel: option: option_instat_callback: error -2
Oct 11 10:14:13	kern	err	kernel: option: option_instat_callback: error -2
Oct 11 10:14:13	kern	err	kernel: option: option_instat_callback: error -2
Oct 11 10:14:13	kern	err	kernel: option: option_instat_callback: error -2
Oct 11 10:14:13	kern	err	kernel: option: option_instat_callback: error -2
Oct 11 10:14:13	kern	err	kernel: option: option_instat_callback: error -2

Figure 127 – Management – Configure System Log

ITEM	DESCRIPTION
Date/Time	The timestamp of the system event.
Facility	The system location in which the event occurred.
Severity	The importance of the event. Note that these correspond to the Log and Display Level settings of the System Log – Configuration page.
Message	A short description of the event.
Refresh button	Click to update the contents of the log since the time the System Log display was opened or since its Refresh button was last pressed.
Close button	Click to close the System Log display.

Management – Security Log

The **Security log** page allows you to view the security log of the gateway and reset its content.

The security log primarily tracks the history of access to, or attempts at accessing, the NL1901ACV gateway.

Click **Reset** to clear the current log. Once reset it will resume recording log in details from that time forward.

You can also click the [here](#) link to save the Security Log to a downloadable file.

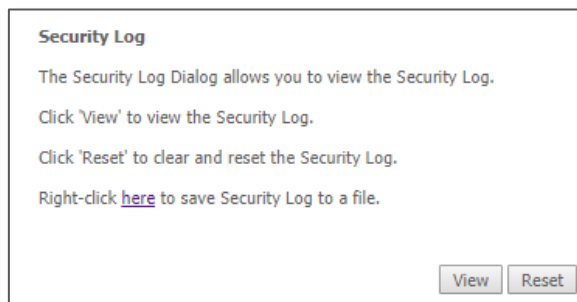


Figure 128 – Management – View Security Log

Click the **View** button to open the **Security Log** in a browser pop up window:

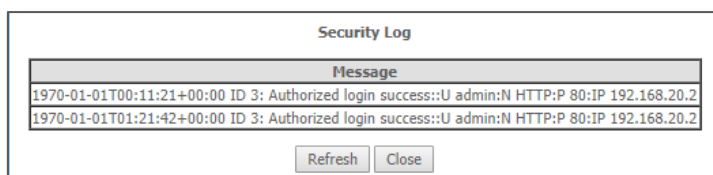


Figure 129 – Management – Download Security Log

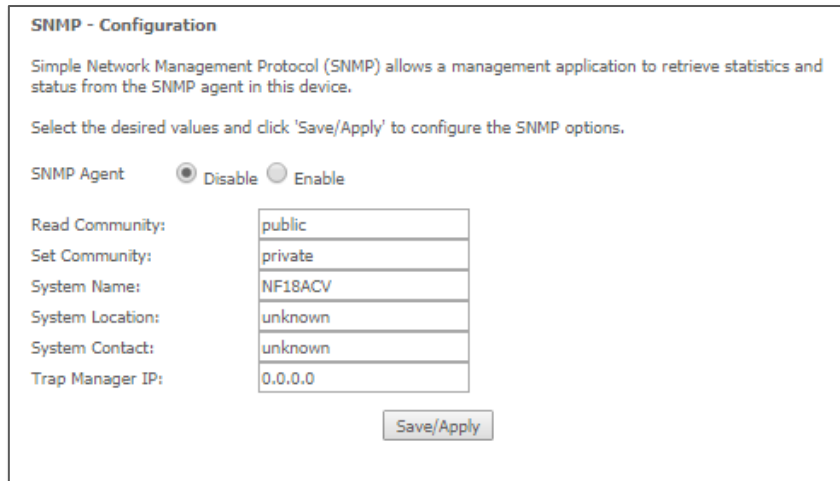
The contains a timestamp and details of logins and login attempts. Details include: Username, Port, IP Address, etc.

Click the **Refresh** button to update the data since the time the **Security Log** display was opened or since its **Refresh** button was last pressed.

Click the **Close** button close the browser pop up window.

Management – SNMP Agent

The **Simple Network Management Protocol (SNMP)** allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the NL1901ACV (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.



SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click 'Save/Apply' to configure the SNMP options.

SNMP Agent ☒ Disable ☐ Enable

Read Community:	public
Set Community:	private
System Name:	NF18ACV
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

Figure 130 – Management – Enable SNMP Agent

Management – TR-069 Client

TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your gateway if supported by your Internet Service Provider (ISP).

By default it is turned off. Go to **Management > TR-069 Client** and select ☒ **Enable WAN Manage Protocol (TR-069)** to enable this service.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click 'Apply/Save' to configure the TR-069 client options.

☒ Enable WAN Management Protocol (TR-069).

Inform ☒ Disable ☐ Enable

Inform Interval: (0~32000000s)

ACS URL:

ACS Username:

ACS Password:

WAN Interface used by TR-069 client: Any_WAN ▼

Display SOAP messages on serial console ☐ Disable ☒ Enable

☒ Connection Request Authentication

Connection Request Username:

Connection Request Password:

Connection Request URL:

Figure 131 – Management – Enable TR-069 Client

Once enabled, the following fields are available.

FIELD	DESCRIPTION
Inform	Select <input checked="" type="radio"/> Enable for the TR-069 client to inform session initialisation of the Auto-Configuration Server (ACS).
Inform interval	Time in seconds that inform session data is sent to the Auto-Configuration Server (ACS). The interval can be up to approximately one year – 32,000,000 seconds.
ACS URL	The address where the ACS server is located.
ACS User Name	The user name to access the ACS server.
ACS Password	The password to access the ACS server.
WAN Interface used by TR-069 Client	The interface connection used to send and receive data to the ACS server.
Display SOAP messages on serial console	Use for troubleshooting via SSH or Telnet.
Connection Request Authentication	Select <input checked="" type="checkbox"/> Connection Request Authentication to add the security of a username and password and identify the URL of the connecting device. When this is selected the following three fields are enabled:
Connection Request Username	Specify the Username required to be entered in order to make a TR-069 connection.

FIELD	DESCRIPTION
Connection Request Password	Specify the Password required to be entered in conjunction with the Connection Request Username
Connection Request URL	Specify the URL of the ACS.
Get RPC Methods button	Remote Procedure Calls (RPC) whose definition determine the types of TR-069 messages that are sent and received by an ACS or CPE. Every RPC is defined in the TR-069 base XML schema which can be found on the Broadband Forum website.
Apply/Save button	Click to save and apply any changes.

Table 46 – TR-069 Client settings table

Management – Internet Time

The tools on this page allow you to use the Network Time Protocol (NTP) to configure specific time servers to synchronise time, set local time zones, etc. for the gateway. The time servers are correct to within a few milliseconds of Coordinated Universal Time (UTC).

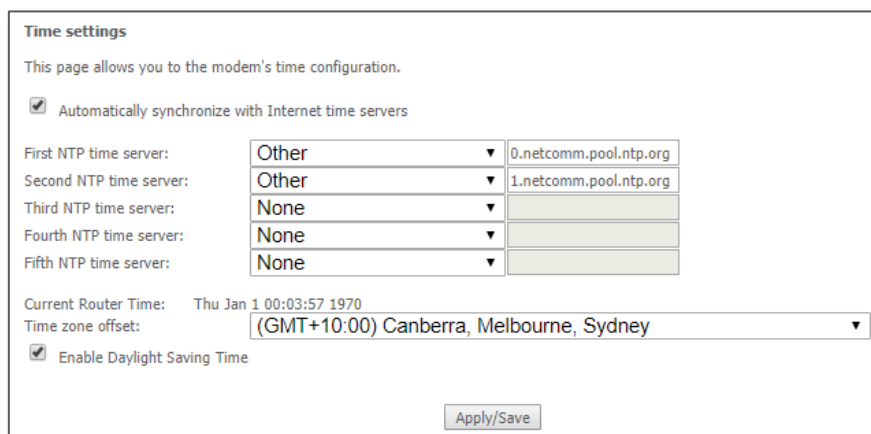





Figure 132 – Management – Internet Time Settings

Drop down to select existing time server to use, or select **"Other"** to manually enter time server. Click the **"Apply/Save"** button to initiate the change.

Management – Access Control

The Access Control option found in the Management drop down menu configures access related parameters in the following three areas:

-  Passwords
-  Access list
-  Services Control

Access Control is used to control local and remote management settings for your gateway.

Passwords

The Passwords option configures your account access username and password for your NL1901ACV gateway. Use the fields illustrated in the screen below to change or create change either the username or the password, or both. Usernames and passwords must be 16 alphanumeric characters or less with no spaces. Both are case sensitive.

Select **Management > Access Control > Passwords** to access these controls.

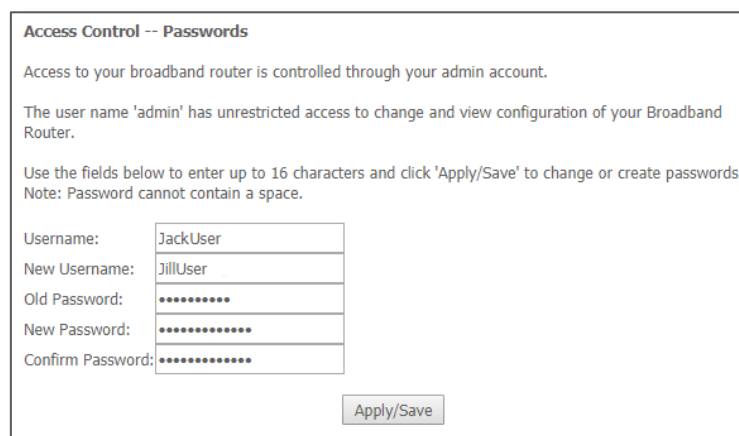


Figure 133 – Access Control – Passwords

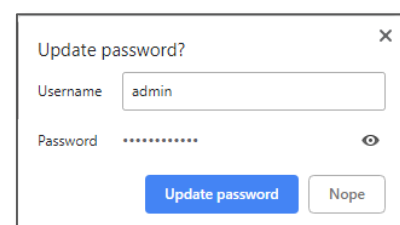
To change the username and/or the password:

- 1 Enter the current password into the **Username** field.
- 2 If you want to change the username, enter the replacement name in the **New Username** field.
If you do not want to change the username, enter the current username in the **New Username** field.
- 3 If you want to change the password, enter the replacement alphanumeric string into the **Old Password** field.
If you do not want to change the password, enter the current password string into the **New Password** field.
- 4 Always enter the same string of characters that are in the **New Password** field into the **Confirm Password** field.
- 5 Click the **Apply/Save** button to make the changes in your access settings.

You will be prompted to login using the new username and/or password.

After successful login you will be prompted to remember the new password.

Click the **Update password** button.



Access List

When this facility is enabled, only those IP addresses in the list can access local management services on the device.

This is used to restrict management access from the internet to the specified IP address.

Access Control -- IP Address The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Access Control Mode: ☐ Disable ☒ Enable

IP Address	Subnet Mask	Remove
123.123.123.123	255.255.255.255	<input type="checkbox"/>

Figure 134 – Access Control – IP Address Access List

To add a device to the list click the **Add** button and then enter its IP Address and Subnet Mask using CIDR slash notation:

123.123.123.123/32

To permanently delete an IP Address from the list, select ☒ in the **Remove** column and then click the **Remove** button.

Services Control

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below and specifying the service port assign to the service.

The following access services are available: FTP, HTTP, ICMP, SAMBA, SNMP, SSH, TELNET, and TFTP.

Click the **Apply/Save** button after making any changes to continue.



Note – You should change your default password, before enabling a WAN service.

Access Control -- Services

Services access control list (SCL) enable or disable the running services.

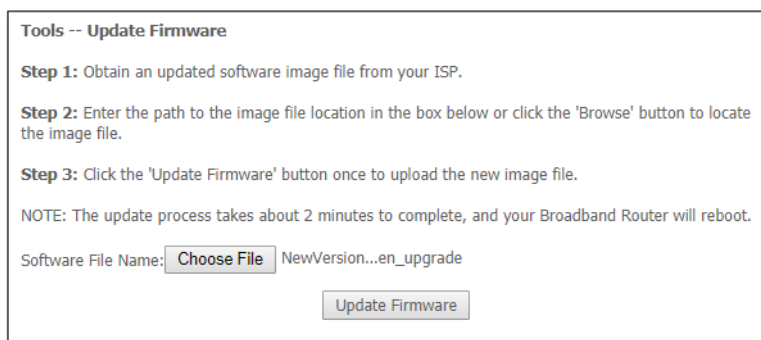
Services	LAN	LAN Port	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	80	<input type="checkbox"/> enable	80
TELNET	<input checked="" type="checkbox"/> enable	23	<input type="checkbox"/> enable	23
SSH	<input checked="" type="checkbox"/> enable	22	<input type="checkbox"/> enable	22
FTP	<input checked="" type="checkbox"/> enable	21	<input type="checkbox"/> enable	21
TFTP	<input checked="" type="checkbox"/> enable	69	<input type="checkbox"/> enable	69
ICMP	<input checked="" type="checkbox"/> enable	0	<input type="checkbox"/> enable	0
SNMP	<input checked="" type="checkbox"/> enable	161	<input type="checkbox"/> enable	161
SAMBA	<input checked="" type="checkbox"/> enable	445	<input type="checkbox"/> enable	445

Figure 135 – Service Control List (SCL)

Management – Update Firmware

The following screen appears when selecting the **Update Firmware** option from the **Management** menu. By following this screen's steps, you can update your gateway's firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

- 1 Obtain an updated software image file from: <http://support.netcommwireless.com/>
- 2 Click the **Choose File** button to locate the image file.
- 3 Click the **Update Firmware** button once to upload and install the file.



Tools -- Update Firmware

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.

Step 3: Click the 'Update Firmware' button once to upload the new image file.

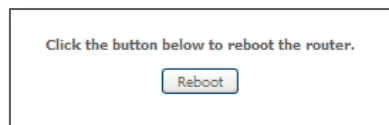
NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: NewVersion...en_upgrade

Figure 136 – Update Firmware page

Management – Reboot

This option reboots the NL1901ACV. Please allow up to 5 minutes for device to reboot.



Click the button below to reboot the router.

Figure 137 – Reboot button



Note 1. – It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings to your Network interface card (NIC).

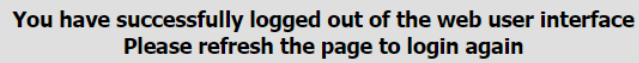


Note 2. – If you lose all access to your web user interface, simply press and hold the reset button on the rear panel for 10 seconds to restore default settings

Logout

Click the **Logout** link to terminate your connection to the NL1901ACV gateway.

The menu on the left margin will disappear and the following message will display in the NL1901ACV web page:



**You have successfully logged out of the web user interface
Please refresh the page to login again**

Figure 138 – Successful log out confirmation message

Reconnect

To re-establish your connection to the gateway, click your browser's  **Reset** button.

The **Sign in** dialog will appear.

Enter your **Username** and **Password** and click the **Sign in** button to reopen the web user interface.

Additional Product Information

Establishing a wireless connection

Windows 7

- 1 Open the **Network and Sharing Center** (Start > Control Panel > Network and Sharing center).
- 2 Click on "**Change Adapter settings**" on the left-hand side.
- 3 Right-click on "**Wireless Network Connection**" and select "**Connect / Disconnect**".
- 4 Select the wireless network listed on your included wireless security card and click **Connect**.
- 5 Enter the network key (refer to the included wireless security card for the default wireless network key).
- 6 You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "**Home**" location.
- 7 You may then see a window prompting you to setup a "**HomeGroup**". Click "**Cancel**" on this.
- 8 You can verify your wireless connection by clicking the "**Wireless Signal**" indicator in your system tray.
- 9 After clicking on this, you should see an entry matching the SSID of your NL1901ACV with "**Connected**" next to it.

Windows 8/8.1/10

- 1 Open the **Network and Sharing Centre** (Click on **Start**, type "**Network and Sharing Centre**")
- 2 Click on "**Change adapter settings**" on the left hand column.
- 3 Right-click on **Wireless Network Adaptor** and select "**Connect / Disconnect**".
- 4 Select the wireless network listed on your included wireless security card and click **Connect**.
- 5 Enter the network key (refer to the included wireless security card for the default wireless network key).
- 6 You can verify your wireless connection by clicking the "**Wireless Signal**" indicator in your system tray.
- 7 After clicking on this, you should see an entry matching the SSID of your NL1901ACV with "**Connected**" under it.

Mac OSX 10.6

- 1 Click on the **Airport** icon on the top right menu.
- 2 Select the wireless network listed on your included wireless security card and click **Connect**.
- 3 On the new window, select "**Show Password**", type in the network key (*refer to the included wireless security card for the default wireless network key*) in the **Password** field and then click on **OK**.
- 4 To check the connection, click on the **Airport** icon and there should be a ☒ tick on the wireless network name.



Note – For other operating systems, or if you use a wireless adaptor utility to configure your wireless connection, please consult the operating system documentation for instructions on establishing a wireless connection.

Troubleshooting

Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful in diagnosing the possible cause of a variety of problems.

Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NL1901ACV power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NL1901ACV and the power source are both turned on and device is receiving sufficient power.
3	Turn the NL1901ACV off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Table 47 – Power LED trouble shooting table

Web Configuration

I cannot access the web configuration pages.

STEP	CORRECTIVE ACTION
1	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
2	Your computer's and the NL1901ACV's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the gateway on the Network Setup page.
3	If you have changed the device's IP address, then enter the new one as the URL you enter into the address bar of your web browser.
4	If you are still not able to access the web configuration pages, reset the gateway to the factory default settings by pressing the reset button for ten (10) seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the NL1901ACV restarts. Navigate to 192.168.20.1 in your web browser and enter "admin" (without the quotes) as the username and password.

Table 48 – Web Configuration – no access trouble shooting table

The web configuration does not display properly.

STEP	CORRECTIVE ACTION
1	Delete the temporary web files and log in again. In Internet Explorer, click Tools , Internet Options and then click the Delete Files... button.
2	When a <i>Delete Files</i> window displays, select Delete all offline content and click OK . Note – Steps may vary depending on the version of your Internet browser.

Table 49 – Web Configuration – no display trouble shooting table

Login Username and Password

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Press and hold the Reset button for 10 seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NL1901ACV restarts.
2	You can now login with the factory default username and password "admin" (without the quotes). Note – It is highly recommended to change the default username and password. Ensure that you store the username and password in a safe place.

Table 50 – Login Username and Password trouble shooting table

WLAN Interface

I cannot access the NL1901ACV from the WLAN or ping any computer on the WLAN.

STEP	CORRECTIVE ACTION
1	Check the WiFi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.
2	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the NL1901ACV and your computer(s) are on the same subnet. You can check the gateways configuration from the Network Setup page.

Table 51 – WLAN Interface trouble shooting table

Appendix: Quality of Service setup example

The following Quality of Service (QoS) settings offer a basic setup example, setting up 2 devices connecting to an NL1901ACV gateway, one with the highest priority for data and the other with the lowest priority for data. All other data packet traffic through the gateway assumes a default best effort setting.

Quality of Service refers to the reservation of bandwidth resources on the NL1901ACV gateway to provide different priorities to different applications, users or data flows or to guarantee a certain level of performance to a data flow.

In this implementation, QoS employs DSCP (Differentiated Services Code Point), a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic.

This example guide sets up QoS with two devices (PC and laptop) connecting via Ethernet cable to an NL1901ACV gateway. One device (PC) is assigned high priority traffic while the other device (laptop) is assigned a low priority. Before Quality of Service can be implemented, the first step involves reserving an IP address for each device, identified by their unique MAC addresses.

Reserving IP addresses

So that QoS settings, custom NAT settings, and parental control settings can be managed for each device, it is necessary to reserve an IP address for each of the devices connecting to the NL1901ACV.

Reserved IP addresses are not required to be within the DHCP server range, however they are required to be within the LAN subnet range:

- 1 Navigate to <http://192.168.20.1> in a web browser.
- 2 When prompted, enter **admin** as both the username and password.
- 3 Select **Advanced Setup > LAN**

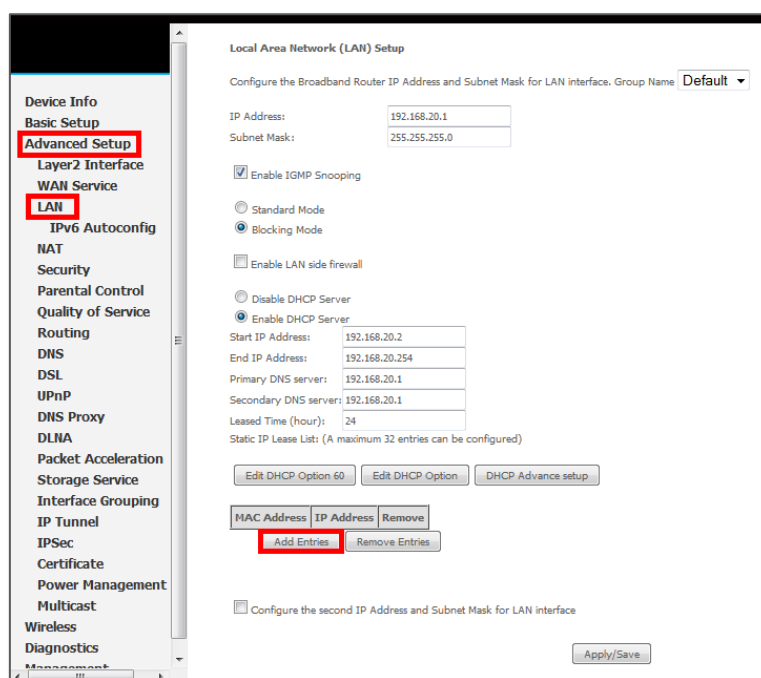
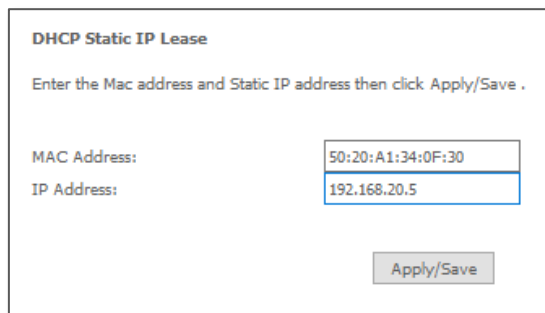


Figure 139 – Advanced Setup > LAN page

- 4 Click the **Add Entries** button.
- 5 Enter the MAC address of the computer/device you are connecting to the gateway. The MAC address is a 12 character set of numbers and letters (A-F), where every 2 characters separated by a colon (:).
- 6 Enter the IP address of the computer/device. This is the local address in the range of 192.168.20.x where x = a number between 2 and 254.



DHCP Static IP Lease

Enter the Mac address and Static IP address then click Apply/Save .

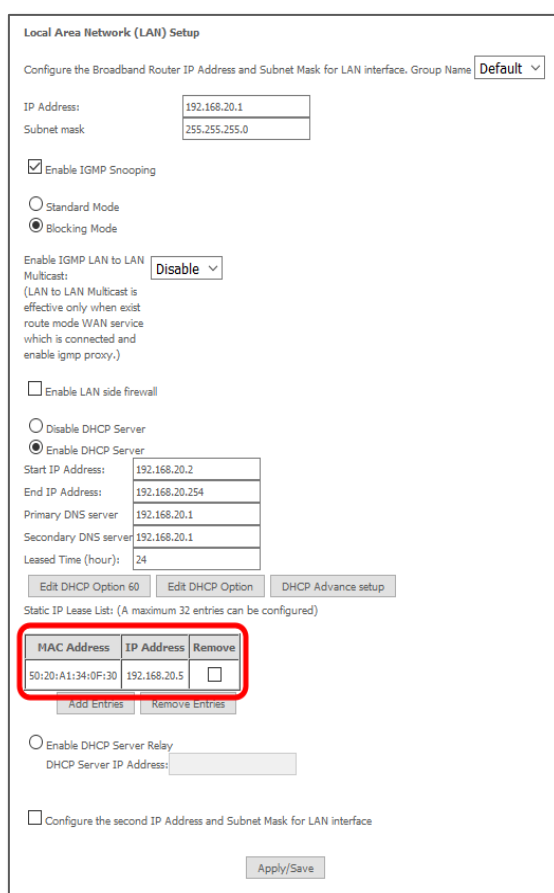
MAC Address: 50:20:A1:34:0F:30

IP Address: 192.168.20.5

Apply/Save

Figure 140 – DHCP Static IP Lease details

- 7 Click the **Apply/Save** button.
- 8 Complete steps 4 through 7 for each device connected to the NL1901ACV gateway. Each entry will be listed in the Static IP Lease List as shown below.



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. Group Name: Default

IP Address: 192.168.20.1

Subnet mask: 255.255.255.0

☒ Enable IGMP Snooping

☐ Standard Mode

☒ Blocking Mode

Enable IGMP LAN to LAN Multicast: Disable

(LAN to LAN Multicast is effective only when exist route mode WAN service which is connected and enable igmp proxy.)

☐ Enable LAN side firewall

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address: 192.168.20.2

End IP Address: 192.168.20.254

Primary DNS server: 192.168.20.1

Secondary DNS server: 192.168.20.1

Leased Time (hour): 24

Edit DHCP Option 60 Edit DHCP Option DHCP Advances setup

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
50:20:A1:34:0F:30	192.168.20.5	<input type="checkbox"/>

Add Entries Remove Entries

☐ Enable DHCP Server Relay

DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

Apply/Save

Figure 141 – LAN Setup

QoS Configuration Settings

- 1 Select **Advanced Setup > Quality of Service**.

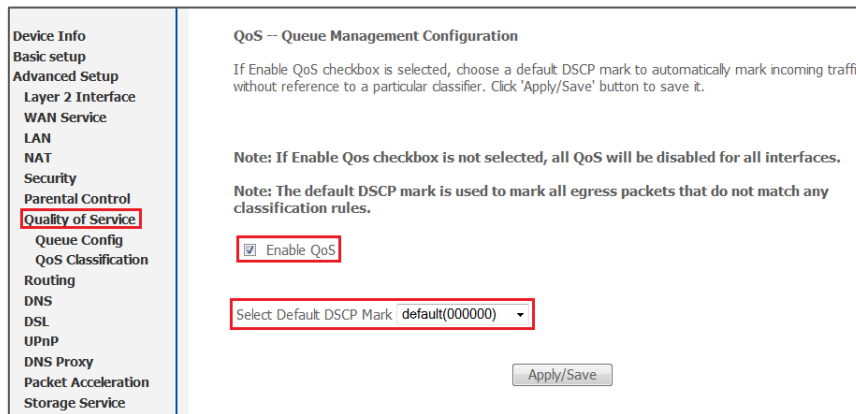
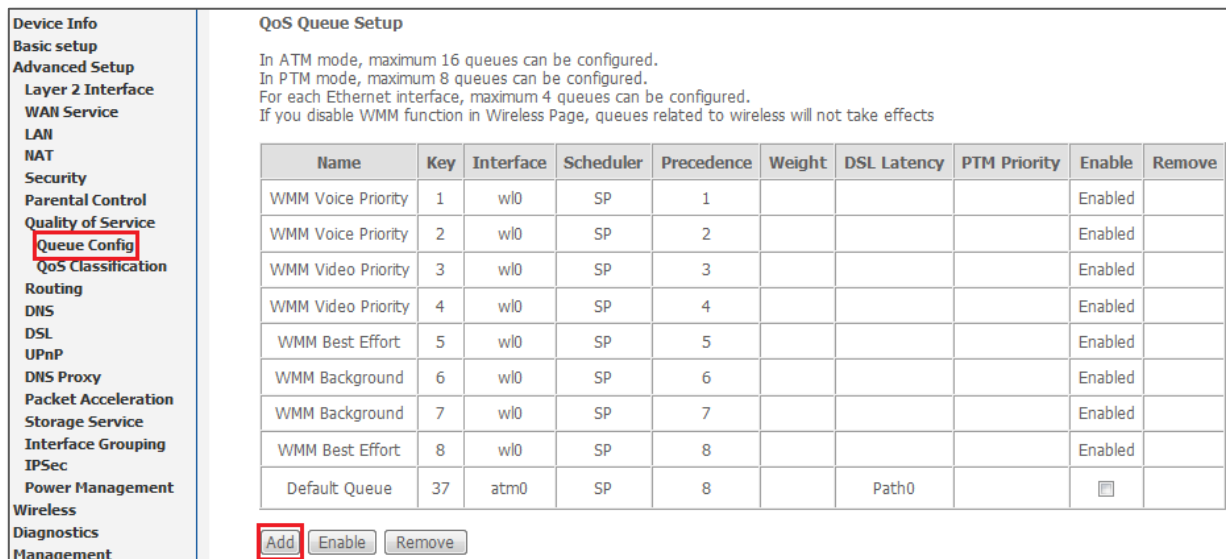


Figure 142 – QoS – Queue Management Configuration

- 2 Select the **Enable QoS** option.
- 3 Select the **Default DSCP Mark** as **default(000000)**.
- 4 Click the **Apply/Save** button.

High Priority QoS Queue Configuration

- 1 Select **Advanced > Quality of Service > QoS Queue > Queue Configuration**.



Name	Key	Interface	Scheduler	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	37	atm0	SP	8		Path0		<input type="checkbox"/>	

Figure 143 – QoS – Queue List

- 2 Click the **Add** button.

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)

- The precedence list shows the scheduler algorithm configured at each precedence level.
 - Note that precedence level with SP scheduler may have only one queue.
 - precedence level with WRR/WFQ scheduler may have multiple queues.

Scheduler Algorithm

☒ Weighted Round Robin
☐ Weighted Fair Queuing

Queue Weight: [1-63]

DSL Latency:

Figure 144 – QoS – Queue Configuration 1

- 3 Enter a **Name** of 15 characters or less to reflect the device that will have high priority QoS, e.g. PC1HighPriority.
- 4 Set the **Enable** option to **Enable**.
- 5 Set the **Interface** (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0_0_100)**).
- 6 Enter a **Queue Precedence**. The lower the value, the higher the priority. For the highest priority, set it to **1(WRR/WFQ)**.
- 7 Select one of the **Scheduler Algorithms**:
 - Ⓐ **Weighted Round Robin** – All services given equal, sequential access.
 - Ⓑ **Weighted Fair Queuing** – More access given to specified services.
- 8 Set the **Queue Weight** from **1** to **63**.
- 9 Set the **DSL Latency** as **Path0**.
- 10 Click the **Save/Apply** button.

Low Priority QoS Queue Configuration

- 1 Select **Advanced > Quality of Service > QoS Queue > Queue Configuration**.
- 2 Click the **Add** button.

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)
- The precedence list shows the scheduler algorithm configured at each precedence level.
- Note that precedence level with SP scheduler may have only one queue.
- precedence level with WRR/WFQ scheduler may have multiple queues.

Queue Weight: [1-63]

DSL Latency:

Figure 145 – QoS – Queue Configuration 2

- Enter a **Name** of 15 characters or less to reflect the device that will have low priority QoS e.g. PC2LowPriority.
- Set the **Enable** option to **Enable**.
- Set the **Interface** (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0)0100**).
- Enter a **Queue Precedence**. The higher the value, the lower the priority. For the lowest priority, set it to **8(WRR)**.
- Set the **DSL Latency** as **Path0**.
- Click the **Save/Apply** button.

High Priority QoS Classification

- Select **Advanced Setup > Quality of Service > QoS Classification**.

Device Info

Basic setup

Advanced Setup

Layer 2 Interface

WAN Service

LAN

NAT

Security

Parental Control

Quality of Service

Queue Config

QoS Classification

Routing

DNS

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA												
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	TOS Check
<div> <input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/> </div>												

Figure 146 – QoS Classification configuration

- Click the **Add** button.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.
Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria A blank criterion indicates it is not used for classification.

Ingress Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Source IP Address[/Mask]:

Destination IP Address[/Mask]:

Differentiated Service Code Point (DSCP) Check:

IP Length Check(Min:Max):

Protocol:

UDP/TCP Source Port (port or port:port):

UDP/TCP Destination Port (port or port:port):

Specify Classification Results (A blank value indicates no operation.)

Specify Egress Interface (Required):

Specify Egress Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a VLAN interface will be tagged with the interface VID and the class rule p-bits.
- Class VLAN packets egress to a VLAN interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit(kbps): [Kbits/s]

Figure 147 – QoS Network High Priority Traffic Class Rule configuration

- 3 Enter a **Traffic Class Name** indicating that it is a high-priority QoS rule, for example: PC1HighPriority
- 4 Leave the **Rule Order** as Last.
- 5 Set the **Rule Status** to Enable.
- 6 Set the **Ingress Interface** according to how the device connects to the gateway. In the example above, LAN is selected. Other options are: Wireless, Local, eth0, eth1, eth2, eth3, eth4.1(routed), wl0/5G or wl1/2.4G
- 7 Set the **Ether Type** to IP(0x800).
Other options include: ARP(0x8086), Ipv6(0x86DD), PPPoE_DISC(0x8863), 8865(0x8865), 8866(0x8866), 8021Q(0x8100)
- 8 Enter the **Source MAC Address** of the device, the unique 12 character signature with every 2 characters separated by a colon(:), that you previously entered to reserve the device's IP address.
- 9 Enter the **Source IP Address** of the device that you previously entered into the Static IP Lease List, in the range of 192.168.1.x In the example above the IP address is: 192.168.20.3
- 10 Enter a **Destination MAC Address** if the connection is to a single device. This is useful for VPN connections. If you wish the destination MAC address to be any address, leave the field blank.
- 11 Enter a **Destination IP Address** if the connection is to a single device. This is useful for VPN connections. If you wish the destination IP address to be any address, leave the field blank.

- 12 Enter a **Destination MAC Mask** if you have entered a Destination MAC address and Destination IP address at steps 10 and 11 above. This would normally be **255.255.255.0** unless your system administrator advises otherwise.
If you have not entered a **Destination MAC** or **IP address**, see steps 10 and 11 above, leave the field blank.
- 13 Set the **Differentiated Service Code Point (DSCP) Check** to: **EF(101110)**
- 14 Set the **Protocol** to **TCP**. Other options include: **UDP, ICMP, IGMP**
- 15 Set "**Assign Classification Queue**" to Priority 1 (in the example above pppoa0&atm0&Path0&Key38&Pre1). Other options or priority 2 and 3. Priority 1 gives the highest priority with priority 3 being the lowest.
- 16 Set **Mark Differentiated Service Code Point (DSCP)** as: **EF(101110)**
- 17 Set **Mark 802.1p Priority** as **5**. In the scale 0-7, 0 is best effort, 6 and 7 are reserved for networking performance so set 5 as the highest priority.
- 18 Enter the **Set Rate Limit** in Kilobits Per Second (kbps).
- 19 Click the **Apply/Save** button.

Low Priority QoS Classification

- 1 Select **Advanced Setup > Quality of Service > QoS Classification**.
- 2 Click the **Add** button.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.
Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

PC1LowPriority

Rule Order:

Last ▼

Rule Status:

Enable ▼

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Ingress Interface:

LAN ▼

Ether Type:

IP (0x800) ▼

Source MAC Address

B4:B6:86:8C:E5:84

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Source IP Address[/Mask]: ▼

192.168.20.3

Destination IP Address[/Mask]:

Differentiated Service Code Point (DSCP) Check: ▼

AF11(001010) ▼

IP Length Check(Min:Max):

Protocol:

TCP ▼

UDP/TCP Source Port (port or port:port):

UDP/TCP Destination Port (port or port:port):

Specify Classification Results (A blank value indicates no operation.)

Specify Egress Interface (Required):

Specify Egress Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP): ▼

AF11(001010) ▼

Mark 802.1p priority:

0 ▼

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.

- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.

- Class non-vlan packets egress to a VLAN interface will be tagged with the interface VID and the class rule p-bits.

- Class VLAN packets egress to a VLAN interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit(kbps):

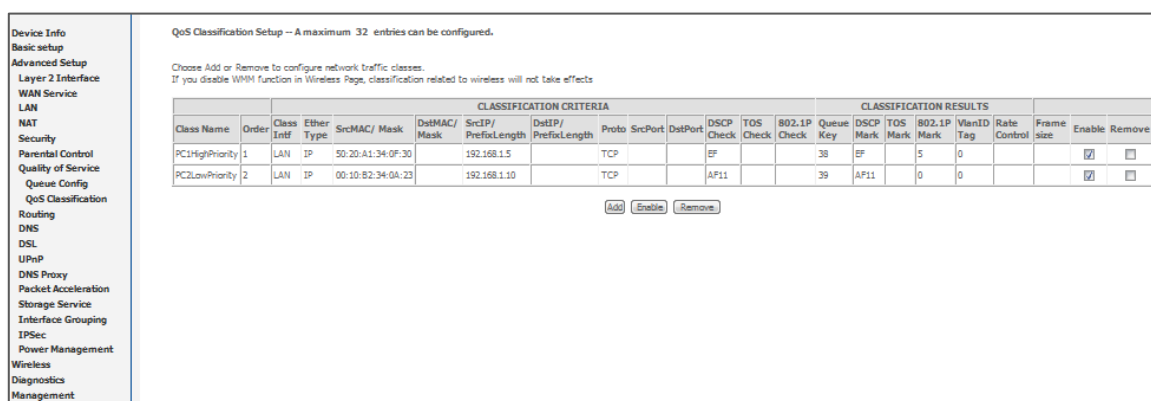
[Kbits/s]

Apply/Save

Figure 148 – QoS Network Low Priority Traffic Class Rule configuration

- 3 Enter a **Traffic Class Name** indicating that it is a low-priority QoS rule, for example: **PC2LowPriority**
- 4 Leave the **Rule Order** as **Last**.
- 5 Set the **Rule Status** to **Enable**.
- 6 Set the **Class Interface** according to how the device connects to the gateway. In the example above **LAN** is selected. Other options are: **Wireless**, **Local**, **eth0**, **eth1**, **eth2**, **eth3**, **eth4.1(routed)**, **wl0/5G** or **wl1/2.4G**
- 7 Set the **Ether Type** to **IP(0x800)**.
Other options include: **ARP(0x8086)**, **Ipv6(0x86DD)**, **PPPoE_DISC(0x8863)**, **8865(0x8865)**, **8866(0x8866)**, **8021Q(0x8100)**
- 8 Enter the **Source MAC Address** of the device, the unique 12 character signature with every 2 characters separated by a colon(:), that you previously entered to reserve the device's IP address.
- 9 Enter the **Source IP Address** of the device that you previously entered into the Static IP Lease List, in the range of 192.168.1.x. In the example above the IP address is: **192.168.20.3**
- 10 Enter a **Destination MAC Address** if the connection is to a single device. This is useful for VPN connections. If you wish the destination MAC address to be any address leave the field blank.
- 11 Enter a **Destination IP Address** if the connection is to a single device. This is useful for VPN connections. If you wish the destination IP address to be any address leave the field blank.
- 12 Enter a **Destination Subnet Mask** if you have entered a Destination MAC address and Destination IP address. This would normally be **255.255.255.0** unless your system administrator advises otherwise.
If you have not entered a **Destination MAC** or **IP address**, see steps 10 and 11 above, leave the field blank.
- 13 Set the **Differentiated Service Code Point (DSCP)** Check to **AF11(001010)**.
- 14 Set the **Protocol** to **TCP**. Other options include **UDP**, **ICMP** or **IGMP**.
- 15 Set "**Assign Classification Queue**" to Priority 3 (in the example above pppoa0&atm0&Path0&Key39&Pre3). Other options are priority 1 and 2. Priority 1 gives the highest priority with priority 3 being the lowest.
- 16 Set **Mark Differentiated Service Code Point (DSCP)** as: **AF11(001010)**
- 17 Set **Mark 802.1p Priority** as **0**. In the scale 0-7, 0 is best effort, 6 and 7 are reserved for networking performance so set 0 as the lowest priority.
- 18 Enter the **Set Rate Limit** in Kilobits Per Second (kbps).
- 19 Click the **Apply/Save** button.

You now have 2 Quality of Service rules implemented for 2 devices connecting to the NL1901ACV gateway.



Device Info
Basic setup
Advanced Setup
Layer 2 Interface
WAN Service
LAN
NAT
Security
Parental Control
Quality of Service
QoS Classification
Routing
DNS
DSL
UPnP
DNS Proxy
Packet Acceleration
Storage Service
Interface Grouping
IPSec
Power Management
Wireless
Diagnostics
Management

QoS Classification Setup – A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS								
Class Name	Order	Class Interface	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	TOS Check	802.1P Check	Queue Key	DSCP Mark	TOS Mark	802.1P Mark	VlanID Tag	Rate Control	Frame size	Enable	Remove
PC1HighPriority	1	LAN	IP	50:20:A1:34:0F:30		192.168.1.5		TCP			EF			38	EF	5	0				<input checked="" type="checkbox"/>	<input type="checkbox"/>
PC2LowPriority	2	LAN	IP	00:10:82:34:0A:23		192.168.1.10		TCP			AF11			39	AF11	0	0				<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Add](#) [Enable](#) [Remove](#)

Figure 149 – QoS Classification setup page

- 20 Select **Management > Reboot**. Click the **Reboot** button to restart the gateway and save the new settings.

- 21 To test your Quality of Service settings try running speed-tests (<http://speedtest.net>) on both PCs/devices simultaneously.

Limiting the upstream rate

- 1 By default, a QoS queue is created when a WAN interface is created but it is disabled by default. On the QoS Queue page, enable the queue for the appropriate WAN interface.

Default Queue	33	atm0	1	8/WRR/1	Path0					<input checked="" type="checkbox"/>	
---------------	----	------	---	---------	-------	--	--	--	--	-------------------------------------	--

Figure 150 – QoS Queue details

- 2 On the QoS Classification page, add a rule to limit the upstream rate, for example:

- Classification Criteria:
- Class Interface: LAN
- Ether type: IP
- Classification Results:
- Class Queue: the queue that was enabled in Step 1
- Set rate-limit: set according to your preference

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Source IP Address[/Mask]:

Destination IP Address[/Mask]:

Differentiated Service Code Point (DSCP) Check:

Protocol:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.

- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.

- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.

- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Figure 151 – Network Traffic Class Rule

- 3 Click **Apply/Save**.

Limiting the downstream rate

- 1 Navigate to the **QoS Queue Configuration** page to add a queue for the LAN interface, for example:

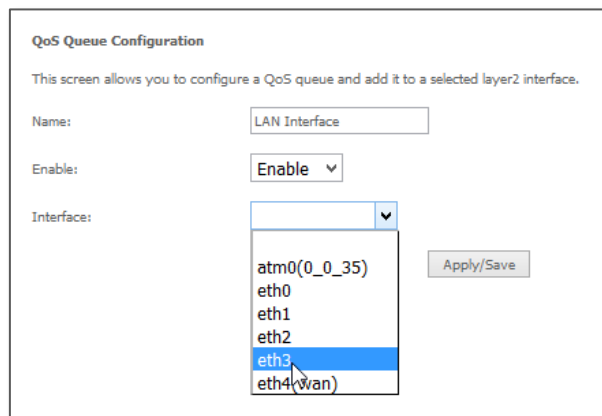


Figure 152 – QoS Queue Configuration

- 1 On the QoS Classification page, add a rule to limit the downstream rate, for example:
 - Classification Criteria:
 - Class Interface: the appropriate WAN interface
 - Classification Results:
 - Class Queue: the queue that was created on Step 1
 - Set rate-limit: set according to your preference

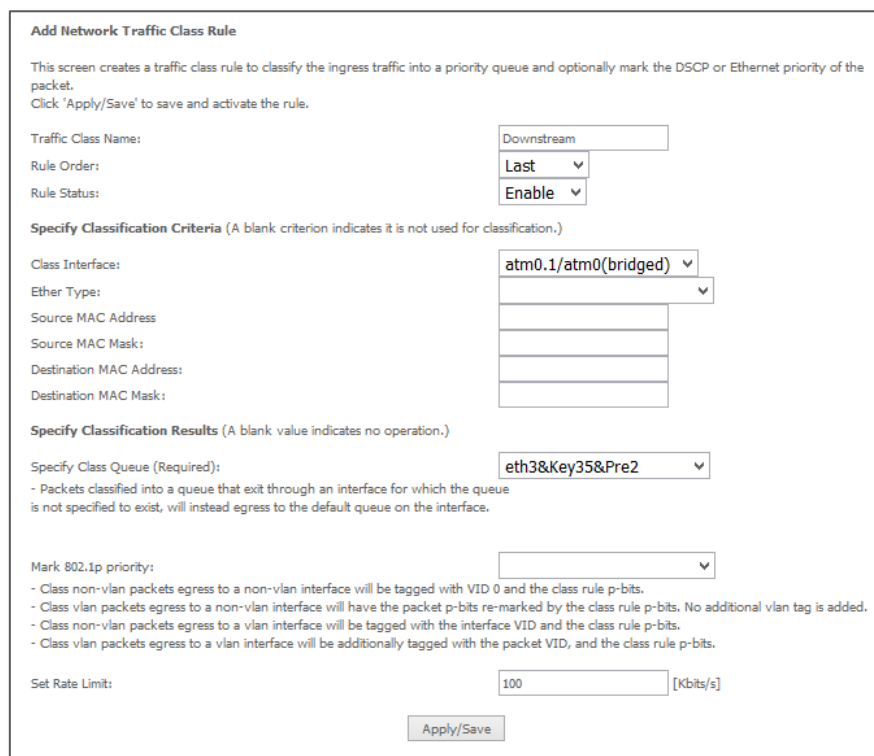


Figure 153 – Network Traffic class Rule

- 2 Click **Apply/ Save**

The QoS Classification table looks like this:

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.

To remove rules, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the rule after page reload.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA												CLASSIFICATION RESULTS								
Class Name	Order	Class Interface	Ethernet Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Prefix Length	Destination IP/Prefix Length	Protocol	Source Port	Destination Port	DSCP Check	TC Check	802.1P Check	Queue Key	DSCP Mark	TC Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove		
Upstream	1	LAN	IP											33				800	<input type="checkbox"/>	<input type="checkbox"/>		
Downstream	2	atm0.1												35				100	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

Figure 154 – QoS Classification list

Table of Figures

Figure 1 – NL1901ACV gateway front view	13
Figure 2 – NL1901ACV gateway rear view	15
Figure 3 – NL1901ACV gateway side view	17
Figure 4 – NL1901ACV gateway – Select Basic Setup	22
Figure 5 – NL1901ACV gateway – Common ADSL setup	23
Figure 6 – NL1901ACV gateway – Select ADSL as WAN connection type	23
Figure 7 – Select PPPoE as WAN mode	24
Figure 8 – Enter PPPoE User ID and Password	24
Figure 9 – NL1901ACV gateway – Common VDSL setup	25
Figure 10 – NL1901ACV gateway – Select VDSL as WAN connection type	25
Figure 11 – Select WAN mode for VDSL connection	26
Figure 12 – Select VLAN option for VDSL connection	26
Figure 13 – VDSL connection – Enter PPPoE User ID and Password	26
Figure 14 – NL1901ACV gateway – Ethernet WAN connection setup	27
Figure 15 – NL1901ACV gateway – Select Ethernet WAN as WAN connection type	27
Figure 16 – Select WAN mode for Ethernet WAN connection	28
Figure 17 – Select VLAN option for PPPoE	28
Figure 18 – Ethernet WAN connection – Enter User ID and Password	28
Figure 19 – IP over Ethernet (IPoE) -- VLAN Setup	29
Figure 20 – IP over Ethernet (IPoE) – Static or Auto IP Address	29
Figure 21 – Unlock PIN code – enter code	30
Figure 22 – NL1901ACV gateway – Device Info section	32
Figure 23 – NL1901ACV gateway – WAN connection status section	33
Figure 24 – NL1901ACV gateway – Cellular Network connection status section	34
Figure 25 – NL1901ACV gateway – WAN Info list	35
Figure 26 – Device Info – Statistics -- LAN display	36
Figure 27 – Device Info – Statistics – WAN Service display	36
Figure 28 – Device Info – Statistics -- xTM display	37
Figure 29 – NL1901ACV gateway	38
Figure 30 – Device Info -- Route list	39
Figure 31 – Device Info -- ARP list	39
Figure 33 – Device Info -- DHCP Leases list	39
Figure 34 – Device Info – CPU & Memory display	40
Figure 35 – DSL ATM Interface list	41
Figure 36 – ATM PVC Configuration page	42
Figure 37 – DSL PTM Interface list	42
Figure 38 – PTM Configuration page	43
Figure 39 – ETH WAN interface list WAN Service	43
Figure 40 – NL1901ACV gateway	44
Figure 41 – WAN Service – Select layer 2 interface	44
Figure 42 – WAN Service – Select WAN Service Type	45
Figure 43 – Enter PPP over Ethernet details	45
Figure 44 – Enter IP over Ethernet details	46
Figure 45 – Enter PPP over Ethernet NAT Translation settings	46
Figure 46 – WAN Setup - Bridging	47
Figure 47 – NL1901ACV Mobile Broadband setup	47
Figure 48 – Mobile Broadband setup interface	49
Figure 49 – SIM – PIN settings	50
Figure 50 – LAN setup -- IPv4 Autoconfig settings	51
Figure 51 – Enter DHCP Static IP Addresses	52
Figure 52 – IPv6 LAN Auto Configuration page	53
Figure 53 – Specify a LAN port for VLAN tagging	54
Figure 54 – NAT -- Virtual Server list	55
Figure 55 – NAT -- Virtual Server Configuration page	55
Figure 56 – NAT -- Port Triggering list	56

Figure 57 – NAT – Port Trigger Configuration page	57
Figure 58 – NAT – DMZ Host settings.....	58
Figure 59 – NAT – Application Layer Gateway (ALG) settings	58
Figure 60 – IP Filtering List – Block outgoing traffic	59
Figure 61 – IP Filtering List – Accept incoming traffic	59
Figure 62 –Outgoing IP Filter settings	59
Figure 63 – Incoming IP Filter settings	60
Figure 64 – Security – MAC Filter list	61
Figure 65 – Security – MAC Filter settings	62
Figure 66 – Advanced – Parental Control – Time Restriction	62
Figure 67 – Advanced – Parental Control – Add Time Restriction.....	63
Figure 68 – Advanced – Parental Control – URL Filter	63
Figure 69 – Advanced – Parental Control – Add URL Filter	64
Figure 70 – Advanced – Enable QoS.....	65
Figure 71 – Advanced – QoS Queue Setup.....	65
Figure 72 – Advanced – QoS – Add QoS Queue	66
Figure 73 – Advanced – QoS – WLAN Queue	66
Figure 74 – Advanced – QoS Classification list	67
Figure 75 – Advanced – QoS – Network Traffic Class settings	67
Figure 76 – QoS Port Shaping settings	68
Figure 77 – Advanced – QoS – Port Shaping settings	68
Figure 78 – Routing – Set Default Gateway	69
Figure 79 – Routing – Static Route list	69
Figure 80 – Routing – Static Route configuration	70
Figure 81 – Routing – Policy Routing list.....	70
Figure 82 – Advanced – Routing – Policy Route configuration.....	70
Figure 83 – Routing – RIP list	71
Figure 84 – DNS Server Configuration.....	72
Figure 85 – Dynamic DNS list	73
Figure 86 – Add Dynamic DNS	73
Figure 87 – DSL settings page	74
Figure 88 – DSL Advanced Settings page.....	75
Figure 89 – ADSL Tone Settings page.....	76
Figure 90 – UPnP activation page	76
Figure 91 – DNS Proxy activation page	77
Figure 92 – DLNA setting page.....	77
Figure 93 – Storage Device Info list.....	78
Figure 94 – Storage User Accounts list.....	78
Figure 95 – Storage User Account Setup page	78
Figure 96 – Interface Grouping list.....	79
Figure 97 – Interface Grouping configuration.....	79
Figure 98 – IPv6inIPv4 Tunnel list	80
Figure 99 – 6in4 Tunnel configuration	80
Figure 100 – IPv4inIPv6 Tunnel list	80
Figure 101 – 4in6 Tunnel configuration	81
Figure 102 – IPSec Tunnel Mode Connections list	81
Figure 103 – IPSec configuration.....	81
Figure 104 – Multicast	83
Figure 105 – Wireless - Basic Configuration.....	86
Figure 106 – Wireless Security.....	87
Figure 107 – Wireless – MAC Filter list	88
Figure 108 – Wireless – MAC Filter configuration.....	88
Figure 109 – Wireless Bridge page.....	89
Figure 110 – Wireless – Advanced configuration page	90
Figure 111 – Wireless – Station Info list.....	94
Figure 112 – Voice Status page	95
Figure 113 – SIP Basic Settings page	96
Figure 114 – Voice- SIP Advanced settings	98
Figure 115 – SIP Extra Setting page.....	102

Figure 116 – SIP Star Code Setting page	103
Figure 117 – SIP Debug Settings page.....	103
Figure 118 – Diagnostics – ETH WAN Diagnostic test results	108
Figure 119 – Diagnostics – Ethernet OAM	110
Figure 120 – Ping IP address	111
Figure 121 – Diagnostics – Traceroute page	111
Figure 122 – Diagnostics – Start/Stop DSL page.....	111
Figure 123 – Settings – Backup page	112
Figure 124 – Settings – Update Settings page.....	112
Figure 125 – Settings – Factory Reset page	113
Figure 126 – Management – View System Log	113
Figure 127 – Management – Configure System Log.....	113
Figure 128 – Management – Configure System Log.....	115
Figure 129 – Management – View Security Log.....	116
Figure 130 – Management – Download Security Log.....	116
Figure 131 – Management – Enable SNMP Agent	117
Figure 132 – Management – Enable TR-069 Client	118
Figure 133 – Management – Internet Time Settings.....	119
Figure 134 – Access Control – Passwords	120
Figure 135 – Access Control – IP Address Access List.....	121
Figure 136 – Service Control List (SCL)	122
Figure 137 – Update Firmware page.....	123
Figure 138 – Reboot button	123
Figure 139 – Successful log out confirmation message.....	124
Figure 140 – Advanced Setup > LAN page.....	128
Figure 141 – DHCP Static IP Lease details	129
Figure 142 – LAN Setup.....	129
Figure 143 – QoS – Queue Management Configuration	130
Figure 144 – QoS – Queue List	130
Figure 145 – QoS – Queue Configuration 1.....	131
Figure 146 – QoS – Queue Configuration 2.....	132
Figure 147 – QoS Classification configuration.....	132
Figure 148 – QoS Network High Priority Traffic Class Rule configuration	133
Figure 151 – QoS Network Low Priority Traffic Class Rule configuration	134
Figure 152 – QoS Classification setup page	135
Figure 153 – QoS Queue details.....	136
Figure 154 – Network Traffic Class Rule.....	136
Figure 155 – QoS Queue Configuration	137
Figure 156 – Network Traffic class Rule	137
Figure 157 – QoS Classification list	138

Table of Tables

Table 1 – Physical dimensions and weight table	11
Table 2 – LAN (Management) table	11
Table 3 – Wireless (WIFI) table	11
Table 4 – NL1901ACV WEB Interface Access table	11
Table 5 – LED indicator table	15
Table 6 – Rear interface table	16
Table 7 – Side interface table	17
Table 8 – Device Info details table	32
Table 9 – WAN connection details table	33
Table 10 – Cellular Network connection details table	34
Table 11 – WAN Info table	35
Table 12 – Statistics -- LAN display table	36
Table 13 – Statistics – WAN Service table	37
Table 14 – Statistics – xTM settings table	37
Table 15 – DSL ATM Interface Configuration settings table	42
Table 16 – USB Mobile configuration settings table	48
Table 17 – DSL ATM Interface Configuration settings table	49
Table 18 – USB mobile PIN Configuration page	50
Table 19 – IPv4 Autoconfig settings table	52
Table 20 – IPv6 LAN Auto Configuration settings	54
Table 21 – NAT -- Virtual Server settings table	56
Table 22 – NAT -- Port Trigger Configuration settings	57
Table 23 – Outgoing IP Filter settings table	60
Table 24 – Incoming IP Filter settings table	61
Table 25 – Advanced – Parental Control – Add Time Restriction Settings	63
Table 26 – Advanced – Parental Control – Add URL Restriction Settings	64
Table 27 – Advanced – Parental Control – Add URL Restriction Settings	65
Table 28 – Routing – Policy Route settings table	71
Table 29 – Routing – RIP settings	71
Table 30 – Routing – RIP settings	73
Table 31 – DSL settings table	74
Table 32 – DSL settings table	75
Table 33 – IPsec settings table	82
Table 34 – Multicast settings table	84
Table 35 – Basic Wireless settings table	86
Table 36 – Wireless security settings table	88
Table 37 – Wireless – Advanced configuration settings	94
Table 38 – SIP settings table	97
Table 39 – VoIP – Advanced – Service Provider settings	101
Table 40 – Dial Plan Syntax table	101
Table 41 – SIP Extra Settings table	102
Table 42 – SIP Debug Settings table	104
Table 43 – Connection to LAN diagnostic test result table	109
Table 44 – Connection to DSL service diagnostic test result table	109
Table 45 – Connection to ISP diagnostic test result table	109
Table 46 – TR-069 Client settings table	119
Table 47 – Power LED trouble shooting table	126
Table 48 – Web Configuration – no access trouble shooting table	126
Table 49 – Web Configuration – no display trouble shooting table	126
Table 50 – Login Username and Password trouble shooting table	127
Table 51 – WLAN Interface trouble shooting table	127

Legal & Regulatory Information

Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out of this Manual are owned by and vest in NetComm (ACN 002490486) (NetComm Limited) (or its licensors). This Manual does not transfer any right, title or interest in NetComm Limited's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm product to which it relates. Otherwise no part of this Manual may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited.

NetComm, NetComm and NetComm Limited are a trademark of NetComm Limited. All other trademarks are acknowledged to be the property of their respective owners.

Customer Information

The Australian Communications & Media Authority (ACMA) requires you to be aware of the following information and warnings:

- 1 This unit may be connected to the Telecommunication Network through a line cord which meets the requirements of the AS/CA S008-2011 Standard.
- 2 This equipment incorporates a radio transmitting device, in normal use a separation distance of 20cm will ensure radio frequency exposure levels complies with Australian and New Zealand standards.
- 3 This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACMA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
 - i Change the direction or relocate the receiving antenna.
 - ii Increase the separation between this equipment and the receiver.
 - iii Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - iv Consult an experienced radio/TV technician for help.
- 4 The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm and legislation of another country's Government may have a similar effect (together these are the Consumer Protection Laws). Any warranty or representation provided by NetComm is in addition to, and not in replacement of, your rights under such Consumer Protection Laws.

If you purchased our goods in Australia and you are a consumer, you are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you purchased our goods in New Zealand and are a consumer you will also be entitled to similar statutory guarantees.

Product Warranty

All NetComm products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a Product Warranty). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm Limited within 30 days of the original purchase date by registering online via the NetComm web site at www.netcommwireless.com. For all Product Warranty claims you will require proof of purchase. All Product Warranties are in addition to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Consumer Protection Laws Section above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section above), the Product Warranty is granted on the following conditions:

- 1 the Product Warranty extends to the original purchaser (you / the customer) and is not transferable;
- 2 the Product Warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
- 3 the customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
- 4 the cost of transporting product to and from NetComm's nominated premises is your responsibility;
- 5 NetComm Limited does not have any liability or responsibility under the Product Warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour; and
- 6 the customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm Limited recommends that you enable these features to enhance your security.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), the Product Warranty is automatically voided if:

- 1 you, or someone else, use the product, or attempt to use it, other than as specified by NetComm Limited;
- 2 the fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
- 3 the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;

- 4 your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
- 5 your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm Limited; or
- 6 the serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitation of Liability

This clause does not apply to New Zealand consumers. Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section above), NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm's liability for breach of that condition or warranty may not be excluded but may be limited, then subject to your rights and remedies under any applicable Consumer Protection Laws which cannot be excluded, NetComm's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Limited doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm Limited doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.

To the extent NetComm Limited is unable to limit its liability as set out above, NetComm Limited limits its liability to the extent such liability is lawfully able to be limited.

Contact

Address: NETCOMM LIMITED Head Office

PO Box 1200, Lane Cove NSW 2066 Australia

Phone: +61(0)2 9424 2070

Fax: +61(0)2 9424 2010

Email: sales@netcommwireless.com

Support: <https://support.netcommwireless.com/>